# EXPLANATORY STATEMENT

## Issued by authority of the Minister for Finance

*Digital ID Act 2024*

*Digital ID Rules 2024*

Section 168 of the *Digital ID Act 2024* (the Digital ID Act) provides that the Minister may, by legislative instrument, make rules prescribing matters required or permitted by the Digital ID Act to be prescribed by the rules, or necessary or convenient to be prescribed for carrying out or giving effect to the Digital ID Act.

The *Digital ID Rules 2024* (the Rules) support the operation of the Digital ID Act which aims to provide individuals with secure, convenient, voluntary and inclusive ways to verify their identity for use in online transactions with government and businesses.

Promoting trust in digital ID services (including the function and operation of the Australian Government Digital ID System (the AGDIS)), including by ensuring less data is shared and stored, and in a more secure way, will also facilitate economic benefits for, and reduce burdens on, the Australian economy.

The purpose of the Rules is to establish a robust and effective legal framework governing the AGDIS, its participants and their obligations as approved to operate in the AGDIS. In particular, the Rules include details on:

- fit and proper person considerations relevant to accreditation and participating in the AGDIS;
- requirements for participating in the AGDIS;
- record keeping obligations for certain entities; and
- arrangements relating to the notification and management of cyber security and digital ID fraud incidents that have occurred in relation to the AGDIS, including information sharing powers for the System Administrator.

The Rules also set out distinct obligations and conditions on accredited entities regarding the use or display of the specified image of Australia's Digital ID Accreditation Trustmark (the digital ID trustmark), as provided for under Chapter 8 of the Digital ID Act.

Entities have been accredited to provide digital ID services since 2019 under the Australian Government's Trusted Digital Identity Framework (TDIF) arrangements, commonly referred to as the TDIF pilot accreditation program. The unlegislated AGDIS has also been in operation since 2019 for government services. TDIF participating entities and participating relying parties have had the option to transition to the legislated AGDIS

under the Digital ID Act. The mechanism for this transition is provided by the *Digital ID (Transitional and Consequential Provisions) Act 2024* and supporting rules.

The Digital ID Act allows the Rules, the *Digital ID (Accreditation) Rules 2024* (the Accreditation Rules), *Digital ID (Accreditation) Data Standards 2024* (the Accreditation Data Standards), and *Digital ID (AGDIS) Data Standards 2024* (the AGDIS Data Standards) to be made. These instruments are collectively referred to as the rules and standards.

Upon the commencement of the Digital ID Act and the Rules, only public sector entities are eligible to participate in the AGDIS. Further rules and standards may need to be made to enable private sector participation in the AGDIS within 2 years following commencement of the Digital ID Act. This could include rules on issues such as redress, interoperability, charging, dispute resolution, liability and holding information outside Australia (data localisation).

Until any rules are made regarding data localisation, existing government policies on transferring information abroad will apply to all Australian Government agencies in the AGDIS, in addition to relevant legal requirements such as Australian Privacy Principle 8 regarding cross-border disclosure of personal information. Government entities operating accredited services must also meet strict data security requirements, such as controls related to storage and protection of personal information, supply chain risk management and cloud service provider operation, as part of the accreditation process set out in the Accreditation Rules.

The Digital ID Act includes consultation requirements under section 169 of the Digital ID Act where the Minister proposes to make or amend rules. While the Digital ID Act had not yet commenced at the time of making the Rules, the Department of Finance (the Department) nevertheless observed these requirements in undertaking consultation.

An exposure draft of the Rules and accompanying consultation materials were released for public consultation from 28 May 2024 to 25 June 2024.

The Department undertook over 30 consultation sessions in the form of webinars, face-to-face roundtables and bilateral meetings with over 250 parties over the 4-week consultation period. The Department received 42 long form submissions and 27 web-form comments from a range of parties including digital ID service providers, industry associations, consumer groups, privacy and inclusion advocates, government agencies and individuals. These built on previous consultations on an earlier exposure draft of the Rules in late 2023.

Before making these Rules, the Minister considered issues raised in consultation responses from stakeholders.

Details of the Rules are set out in **Attachment A**.

The Rules are a legislative instrument for the purposes of the *Legislation Act 2003*.

The Rules rely on section 4 of the *Acts Interpretation Act 1901*, as they are made in contemplation of commencement of section 168 of the Digital ID Act. The Rules commence at the same time as the Digital ID Act.

The Office of Impact Analysis (OIA) has been consulted in relation to the Rules and an Impact Analysis **is not required** as these rules do not create any additional impact other than what has already been assessed in the Impact Analysis for the Digital ID Act. OIA reference number: OBPR23-04323.

A Statement of Compatibility with Human Rights is at **Attachment B**.

The Rules are compatible with human rights, and to the extent that they may limit human rights, those limitations are reasonable, necessary and proportionate.

**ATTACHMENT A**

**Details of the *Digital ID Rules 2024***

# Chapter 1—Preliminary

### Rule 1.1 Name

1.1 This rule provides that the name of these rules is called the *Digital ID Rules 2024* (the Rules).

### Rule 1.2 Commencement

1.2 The Rules commence at the same time as the Digital ID Act commences.

### Rule 1.3 Authority

1.3 The Rules are made under section 168 of the Digital ID Act for the purposes of the provisions in the Digital ID Act where the term 'Digital ID Rules' occurs.

1.4 Section 168 of the Digital ID Act enables the Minister to make legislative instruments, such as the Rules.

### Rule 1.4 Definitions

1.5 This rule sets out the definition of a number of expressions in the Rules. Notes 1 and 2 under rule 1.4 relevantly provide that a number of expressions in the Rules are defined in the Digital ID Act or the Accreditation Rules, respectively.

1.6 Some expressions are defined within the rule itself, where those definitions may be the outcome of several requirements and apply in context of the requirements.

# Chapter 2—Fit and proper person considerations

### Rule 2.1 Application of this Chapter

2.1 Subrule 2.1(1) provides that, for the purposes of paragraph 12(a) of the Digital ID Act, Chapter 2 specifies the matters to which the Digital ID Regulator must have regard when considering if the person is a fit and proper person for the purposes of the Digital ID Act, the Rules, the Accreditation Rules, the Accreditation Data Standards and the AGDIS Data Standards. These matters are specified in rule 2.2 of Chapter 2.

2.2 A Note to subrule 2.1(1) explains that the Digital ID Regulator may have regard to whether an entity is a fit and proper person 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 (AGDIS), or suspend or revoke the approval of an entity to participate in the AGDIS. The note refers to subsections 15(5), 25(4), 26(3), 62(2), 71(3) and 72(3) of the Digital ID Act.

2.3 Subrule 2.1(2) relevantly provides that Chapter 2 does not limit the matters to which the Digital ID Regulator may have regard when considering whether the entity is a fit and proper person for the purposes of the Digital ID Act, the Rules, the Accreditation Rules, the Accreditation Data Standards and the AGDIS Data Standards.

### Rule 2.2 Mandatory relevant matters

2.4 Subrule 2.2(1) relevantly provides that in having regard to whether an entity is a fit and proper person, the Digital ID Regulator must have regard to the matters specified in this provision. This includes if the entity or an ***associated person***, as defined in rule 1.4, of the entity has:

- been convicted or found guilty of a serious criminal offence or an offence of dishonesty within the previous 10 years in Australia or a foreign jurisdiction;
- been found to have been in breach of Australian or foreign laws relating to the management of its ***DI data environment***, as defined in rule 1.4;
- engaged in conduct or practices that have been determined to have breached Australian or foreign privacy laws;
- a history of insolvency or bankruptcy; and
- been required to pay compensation for a breach of Australian privacy or consumer law.

2.5 If the entity is a body corporate, the Digital ID Regulator must also have regard to whether any of the directors or associated persons of the entity have been disqualified from managing corporations, or are subject to a banning order.

2.6 Additionally, under subrule 2.2(1) the Digital ID Regulator must consider if the entity has previously been refused an application for accreditation or for approval to participate in the AGDIS. If the entity was accredited or approved to

participate, then the Digital ID Regulator must consider if the entity's accreditation or approval is, or has been, suspended or revoked.

2.7 Subrule 2.2(2) provides that the mandatory relevant matters for a fit and proper person assessment does not affect the operation of Part VIIC of the *Crimes Act 1914* or a corresponding provision of an Australian law or a law of a foreign country.

2.8 The effect of this provision is that subrule 2.2(1) does not affect the operation of an Australian or overseas 'spent conviction' law where the record of the matter has been statutorily removed under that law. A Note to this subrule explains that the *Crimes Act 1914* includes provisions which, in certain circumstances, relieve persons from the requirement to disclose spent convictions and require persons aware of such convictions to disregard them.

2.9 Subrule 2.2(3) provides for a definition of ***banning order***, ***director*** and ***serious criminal offence*** for use in rule 2.2. A Note to this subrule explains that the Commonwealth has control over criminal law in the Jervis Bay Territory, which is relevant to the definition of serious criminal offence in this subrule, providing context where the term appears in subparagraph 2.2(1)(a)(i).

# Chapter 3—Participation in the Australian Government Digital ID System

# Part 1—Applications for approval to participate

### Rule 3.1 Application of this Part

3.1 This rule refers to paragraph 62(1)(f) of the Digital ID Act, which provides that the Rules may prescribe requirements for entities seeking approval from the Digital ID Regulator to participate in the AGDIS.

3.2 Rule 3.1 outlines that this Part prescribes additional requirements that must be met before the Digital ID Regulator may approve an entity to participate in the AGDIS.
A Note to rule 3.1 explains that an application made under section 61 of the Digital ID Act (application for approval to operate in the AGDIS) must be accompanied by any information or documents required by this Part.

3.3 This Note explains that for the purposes of an application made under section 61, paragraph 141(1)(c) of the Digital ID Act states that an application made under the Digital ID Act must be accompanied by any information or documents required by the Rules or the Accreditation Rules.

3.4 This Note also explains that under subsection 143(2) of the Digital ID Act, the Digital ID Regulator is not required to make a decision on an application until the information or documents are provided.

### Rule 3.2 Applications for approval to participate—all entities

3.5 This rule sets out criteria that must be met by all entities seeking to participate in the AGDIS.

3.6 This rule provides for the Digital ID Regulator to be satisfied that an entity has effective written procedures in place to notify the System Administrator of:

- any proposed changes to the entity's IT system that interacts with the AGDIS; or
- any planned or unplanned IT system outages or downtime,

if these events will or could reasonably be expected to have a material effect on the operation of the AGDIS.

3.7 The Digital ID Regulator must be satisfied of this requirement before approving an application to participate in the AGDIS.

3.8 The term ***material effect*** is defined in rule 1.4 in relation to the operation of the AGDIS. It includes any degradation or loss of functionality within the AGDIS, and any detrimental effect on the ability of an entity that participates in the AGDIS to access the AGDIS.

3.9 Circumstances that could meet the threshold of having a 'material effect' on the AGDIS include incidents that may or will cause the degradation or loss of

functionality within the AGDIS, or anything that could or would have a detrimental effect on the ability of an entity participating in the AGDIS to access the AGDIS. The matters to be considered are non-exhaustive and entities may seek to include in their written procedures some parameters or considerations to support internal decision-making on determining what would constitute a material effect that will require notification.

3.10 Where a material effect on the AGDIS has been identified, entities should have procedures in place to enable notification to the System Administrator as soon as practicable. The policy intent is for entities to provide any notifications of material effect without delay, once it is reasonably feasible to do so.

3.11 The AGDIS operates as a 'federated' system, which means that the operations of some parties can affect other parties in the AGDIS. For example, certain changes made to the IT environment of an accredited entity may impact the availability of services provided to participating relying parties in the AGDIS. Further, operational issues experienced by participating relying parties could trigger customer enquiries to accredited entities or the System Administrator, which could impact the ability of these entities to respond efficiently and effectively in those circumstances.

3.12 This rule establishes a relationship between the System Administrator and all entities participating in the AGDIS, providing the System Administrator with a full view of the AGDIS. This will enable the System Administrator to effectively coordinate and respond to incidents, including proposed changes to, and outages affecting, entities' information technology (IT) systems, across the federated AGDIS.

3.13 The rule requires the Digital ID Regulator to be satisfied that an entity has effective written procedures in place before approving an application for approval to participate in the AGDIS. The Digital ID Regulator is empowered under subsection 142(1) of the Digital ID Act to require, by written notice, that an applicant give information or documents to assist in the consideration of their application. The Digital ID Regulator is not required to make a decision on an application if this subsection is not complied with (subsection 143(3) of the Digital ID Act refers).

**Rule 3.3 Applications for approval to participate—relying parties**

3.14 This rule sets out requirements for entities seeking to apply for approval to participate in the AGDIS as relying parties (relying party applicant). These requirements are based on pre-existing requirements under the TDIF applying to Government entities seeking to onboard to the AGDIS and recognise the possible impact that ineffective management of particular incidents may have on the entities and services in the federated AGDIS. The rule is designed to ensure the Digital ID Regulator and relying party applicants have a common understanding, prior to approving a relying party's application for approval to participate in the AGDIS, as to how to manage particular incidents in order to resolve them as effectively as possible.

3.15 Subrule 3.3(1) requires relying party applicants to conduct a risk assessment which identifies, evaluates and manages possible risks of a cyber security or digital ID fraud incident which may occur in connection with a service the entity intends to provide, or provide access to, within the AGDIS.

3.16 Subrule 3.3(2) relevantly provides that a relying party applicant must have certain written plans in place at the time of applying for approval to participate in the AGDIS: a cyber security plan; a digital ID fraud management plan; and a disaster recovery and business continuity plan. These plans must be in writing, approved by an entity's governing body, and reviewed at least annually. Paragraphs 3.3(2)(a), (b) and (c) set out other requirements for these plans.

3.17 As with rule 3.2, the Digital ID Regulator is empowered under subsection 142(1) of the Digital ID Act to require, by written notice, that a relying party applicant give information or documents to assist in the consideration of their application. The Digital ID Regulator is not required to make a decision on an application if this subsection is not complied with (subsection 143(3) of the Digital ID Act refers).

# Part 2—Approval to participate

### Rule 3.4 Conditions on approval to participate

3.18 This rule sets out conditions made for the purposes of subsection 64(5) of the Digital ID Act.

3.19 Subsection 64(5) of the Digital ID Act provides that the Rules may determine that the approval of each entity, or of each entity included in a specified class, to participate in the AGDIS is subject to one or more specified conditions.

3.20 Subrule 3.4(1) sets out a table of participation conditions for entities approved to participate in the AGDIS. The table approves an entity, listed in column 1, to participate in the AGDIS, but that participation is subject to the conditions, listed in column 2.

3.21 The conditions in this table apply variously to participating relying parties and accredited exchange providers.

3.22 Items 1 to 3 of the table relate to notification requirements for participating relying parties.

3.23 Item 1 requires a participating relying party to notify the Digital ID Regulator of a proposed change to its contact details no later than 7 days after the change takes effect.

3.24 Item 2 requires a participating relying party to notify the System Administrator of particular types of incidents in relation to its IT system (such as changes, outages or downtime, whether planned or unplanned) that will or could reasonably be expected to have a material effect on the operation of the AGDIS. A notification must be made no later than 5 business days after the entity becomes aware of the incident, or the entity reasonably suspects that the incident has occurred, whichever comes earlier.

3.25 Item 3 requires a participating relying party to collect and store the pairwise identifier issued to the relying party by an identity exchange provider (IXP) in

relation to each individual accessing the relying party's services. This is to enable the participating relying party to comply with paragraph 4.2(3)(k), which relates to notifications of cyber security incidents and digital ID fraud incidents. The term ***pairwise identifier*** is defined in Rule 1.4 of the Rules. As a privacy-enhancing feature, the pairwise identifier prevents an individual from being linked or tracked across parties by using separate transaction identifiers for an accredited entity and a participating relying party that are not shared between parties to the transaction.

3.26 Subrule 3.4(2) sets out information that must be included in notifications if a notification is required by a participating relying party under items 1 and 2 of the participation conditions table. Under section 133 of the Digital ID Act, the Digital ID Regulator also has the power to require further information or documents from entities where it reasonably believes that an entity has, or may have, information or documents relevant to the entity's compliance under the rules and standards, or to the functions and powers of the Digital ID Regulator.

# Chapter 4—Reportable incidents

### Rule 4.1 Application of this Chapter

4.1 Subsection 78(1) of the Digital ID Act states that the Rules may prescribe arrangements relating to the notification and management of reportable incidents that have occurred, or are reasonably suspected of having occurred, in relation to the AGDIS.

4.2 Incident reporting requirements will enable the Digital ID Regulator and the System Administrator to coordinate and promptly manage responses to incidents that may affect, are likely to affect, or have affected the security, integrity or performance of the AGDIS. This will help build trust in the AGDIS.

4.3 This rule provides that Chapter 4 prescribes arrangements relating to reportable incidents.

4.4 A Note to rule 4.1 provides that an entity is liable to a civil penalty if the entity is subject to a requirement under this Chapter and fails to comply with the requirement. The civil penalty provision is set out in subsection 78(4) of the Digital ID Act. The liability of entities to civil penalties demonstrates the importance of compliance with incident reporting requirements to uphold the stability, security and integrity of the AGDIS.

### Rule 4.2 Cyber security incidents and digital ID fraud incidents

4.5 This rule sets out notification requirements for certain entities where a cyber security incident or digital ID fraud incident occurs or is reasonably suspected of having occurred. These types of incidents are defined in section 9 of the Digital ID Act.

4.6 The rule is designed to enable the System Administrator to perform its functions in promoting the performance and integrity of the AGDIS. The threshold for notification, as well as the form and timing of such notification, has been developed having regard to the number of parties that may be involved in a digital ID transaction within the AGDIS, and therefore the necessity for the System Administrator to take prompt action in coordination of a response and determine which party is best placed to respond to the incident.

4.7 Subrule 4.2(1) provides that this rule applies to participating entities, including those entities who have been approved to participate in the AGDIS but their approval to participate has been suspended by the Digital ID Regulator. It also applies to entities whose approval to participate has been revoked by the Digital ID Regulator, in relation to incidents that have occurred, or are reasonably suspected of having occurred, while that entity was participating in the AGDIS.

4.8 Subrule 4.2(2) establishes the threshold for notification to the System Administrator in relation to a cyber security incident or digital ID fraud incident. An entity must notify the System Administrator of any incident that is a cyber security incident or digital ID fraud incident.

4.9 In order to meet the threshold for notification, the relevant incident must have occurred, or be reasonably suspected of having occurred, in relation to accredited services within the AGDIS. For accredited entities, this means accredited services provided within the AGDIS, and for participating relying parties, this means accredited services received within the AGDIS.

4.10 For example, incidents that could meet the definition of digital ID fraud incident in the Digital ID Act, and be required to be notified to the System Administrator, could be where a digital ID used within the AGDIS has been compromised, or where a digital ID is created in the AGDIS that does not correspond to a real person. As such an incident could impact numerous other parties operating in the AGDIS, the System Administrator should be notified of the actual or suspected incident to enable a coordinated incident response.

4.11 Subrule 4.2(3) sets out the information that a notification must include. This information will enable the System Administrator to take necessary action in incident coordination and management.

4.12 Subrule 4.2(4) requires entities to notify the System Administrator as soon as practicable after, and in any event no later than one business day after, becoming aware of the incident or suspected incident.

4.13 Subrule 4.2(5) permits an entity to notify the System Administrator orally. However, if an entity notifies orally, the entity must give a written notification no later than 3 business days after the oral notification. The provision for oral notification recognises the pace and resources required to effectively identify and respond to suspected or actual cyber security or digital ID fraud incidents.

4.14 Subrule 4.2(6) sets out the notification requirements for an entity where both of the following applies:

- the entity is not able to comply with the requirements in subrules 4.2(3) – (5), relating to the information that must be included in the notification and the timeframes and form in relation to that notification; and
- the entity is not able to comply with these requirements because it is not reasonably practicable to do so.

4.15 An entity will need to provide an interim written notification within one business day (or 3 business days if given orally) with as much of the required information as is reasonably available to the entity at the time the interim notification is given. The entity must take reasonable steps to obtain the outstanding information as soon as reasonably practicable and provide the outstanding information to the System Administrator as soon as reasonably practicable, and in any event, within 48 hours of the outstanding information becoming available to the entity.

4.16 As outlined in the Note to rule 4.1, an entity that fails to comply with this rule is liable to a civil penalty. In addition, should an entity not comply with the notification requirements, it may be a relevant consideration for the Digital ID Regulator in the exercise of its powers under the Digital ID Act to vary, suspend or revoke an entity's approval to participate in the AGDIS (sections 70, 71 and 72 of the Digital ID Act refer). However, these notification requirements are not

designed to be punitive or act as a deterrent to participation in the AGDIS. Rather, they are intended to enable prompt, coordinated and effective response to incidents that may or will impact the operation of the AGDIS.

**Rule 4.3 Other incidents**

4.17 Subrule 4.3(1) outlines that this rule relates to incidents that have occurred, or are reasonably suspected of having occurred, while an entity was participating in the AGDIS. It sets out the requirements that apply to participating entities, including those entities who have been approved to participate in the AGDIS but that approval to participate has been suspended by the Digital ID Regulator.

4.18 Subrule 4.3(2) provides for other types of incidents that an entity must notify to the Digital ID Regulator. An entity must notify the Digital ID Regulator:

- of any material change in the entity's circumstance that might affect its ability to comply with obligations under the Digital ID Act, the Rules, the Accreditation Rules, the Accreditation Data Standards and the AGDIS Data Standards;
- where it has identified any matter that could reasonably be considered relevant to whether the entity is a fit and proper person for the purposes of the Digital ID Act, the Rules, the Accreditation Rules, the Accreditation Data Standards and the AGDIS Data Standards; and
- of any material change to, or error in, any information provided to the Digital ID Regulator.

4.19 The policy intent is for the entity to provide notification in relation to changes in an entity's circumstances that is significant enough to influence an entity's compliance with the Digital ID Act. This could, for example, be in relation to possible non-compliance with the Rules, or the AGDIS Data Standards, and maintenance of agreed performance or quality within the AGDIS. Such circumstances could also be relevant to the Digital ID Regulator's consideration as to whether the entity is a fit and proper person to be approved to participate in the AGDIS (within the meaning of Chapter 2 of the Rules and paragraph 12(a) of the Digital ID Act).

4.20 Subrule 4.3(3) provides for certain types of incidents that an accredited entity must notify to the System Administrator. An accredited entity must notify the System Administrator of any proposed change to its IT system that interacts with the AGDIS, where that change will, or could reasonably be expected to, have a material effect on the operation of the AGDIS. Additionally, an accredited entity must provide a notification of any outage of downtime affecting its IT system (whether planned or unplanned), in instances where the outage or downtime will, or could reasonably be expected to, have a material effect on the operation of the AGDIS. These reporting requirements will enable the System Administrator to take appropriate action to protect the security, integrity or performance of the AGDIS.

4.21 Subrule 4.3(4) sets out the information that a notification must include. This information will enable the Digital ID Regulator or System Administrator (depending on the type of incident notification) to exercise their functions.

4.22 Subrule 4.3(5) provides that a notification to the Digital ID Regulator or System Administrator must be made no later than 5 business days after the entity becomes aware of the incident or the entity reasonably suspects that the incident has occurred, whichever comes earlier.

**Rule 4.4 Other digital ID systems**

4.23 Subrule 4.4(1) provides that this rule applies to accredited entities holding approval to participate in the AGDIS, and accredited entities who have had their approval to participate in the AGDIS suspended.

4.24 Subrule 4.4(2) provides that the Digital ID Regulator must be notified if an entity uses an IT system to provide services within the AGDIS, and the entity proposes to use that same IT system to either provide or receive services within a different digital ID system than the AGDIS (***other digital ID system***, see subrule 4.4(5) below).

4.25 Subrule 4.4(3) sets out the information that a notification must include. The details that entities are required to provide will enable the Digital ID Regulator to understand the information flows and interactions between the AGDIS and any other digital ID system involving the accredited entity. This will also better enable the Digital ID Regulator to take necessary action if concerns are raised regarding the interactions between digital ID systems.

4.26 Subrule 4.4(4) provides that a notification must be made no later than 28 days before the entity's proposed participation in the other digital ID system.

4.27 Subrule 4.4(5) clarifies that, for the purposes of this rule, the term ***other digital ID system*** means a digital ID system other than the AGDIS, as set out in paragraph 4.4(2)(b). The definition of digital ID system is set out in section 9 of the Digital ID Act.

**Rule 4.5 System Administrator may give information**

4.28 This rule provides that the System Administrator may give information notified under rule 4.2 or subrule 4.3(3) to the Digital ID Regulator, the Minister or to a participating entity.

4.29 Rule 4.2 provides that participating entities must notify the System Administrator of actual or suspected cyber security incidents and digital ID fraud incidents in relation to their accredited services. Subrule 4.3(3) provides that accredited entities must notify the System Administrator of particular incidents relating to their IT system, including proposed changes, or planned or unplanned outages or downtime.

4.30 A Note to subrule 4.5(1) explains that those notifications relate to cyber security incidents and digital ID fraud incidents, proposed changes to the entity's IT system and planned or unplanned outages or downtime affecting the entity's IT system.

4.31 The purpose of this subrule is to allow for the Digital ID Regulator and the Minister to receive information held by the System Administrator in relation to the operation of the AGDIS.

4.32 Subrule 4.5(2) provides that 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. For example, where a fraudulent digital ID has been identified, or a legitimate digital ID was compromised, the System Administrator may notify the participating relying parties involved in these incidents. The intent is to prevent or minimise the ongoing use of suspicious or compromised digital IDs.

4.33 Subrule 4.5(3) sets out the parameters around when the System Administrator can give information under rule 4.5. This rule provides that 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 AGDIS. A Note to subrule 4.5(3) states that this subrule does not limit the functions of the System Administrator under the Digital ID Act in relation to information-sharing.

4.34 The intent is for the System Administrator to consider giving information under this rule where it is appropriate or necessary for the Digital ID Regulator or Minister to have regard to this information in order to perform their functions or exercise their powers under the Digital ID legislative framework. The Digital ID Regulator has the function of overseeing and maintaining the AGDIS, as well as ensuring regulated entities remain in compliance with their obligations. If the System Administrator becomes aware of information via a notification that is relevant or pertinent to the performance of the Digital ID Regulator's function, this subrule will enable sharing of such information.

4.35 For example, the System Administrator could share information with the Digital ID Regulator that is relevant to an ongoing investigation by the Digital ID Regulator about whether an accredited entity participating in the AGDIS remains suitable to hold accreditation and approval to participate in the AGDIS.

4.36 Subrule 4.5(4) provides that, for the purposes of paragraph 78(2)(g) of the Digital ID Act, a person or body to whom the System Administrator may give information under rule 4.5, is deemed to be authorised to collect this information. Paragraph 78(2)(g) of the Digital ID Act provides that, without limiting subsection 78(1), the Rules may make provision in relation to authorising the collection of information relating to reportable incidents by the Minister, the Information Commissioner, accredited entities, participating relying parties, or other specified bodies.

4.37 A Note to subrule 4.5(4) states that this rule does not limit the functions of the Digital ID Regulator under the Digital ID Act in relation to information-sharing.

# Chapter 5—Trustmarks

### Rule 5.1 Application of this Chapter

5.1 The digital ID trustmark (also known as the Digital ID Accreditation Trustmark) is defined in subsection 117(2) of the Digital ID Act to mean a mark, symbol, logo or design set out in the Rules.

5.2 The digital ID trustmark is a visual indicator designed to give Australian consumers and businesses confidence that a digital ID service is accredited and meets Australian Government standards, is subject to additional privacy safeguards in the Digital ID Act, and so can be trusted by consumers and the businesses.

5.3 Further rules may be made to prescribe other trustmarks in the future, as required.

5.4 Subrule 5.1(1) provides that, for the purpose of subsection 117(1) of the Digital ID Act, this Chapter sets out the digital ID trustmark that accredited entities may use, as well as any conditions and requirements that accredited entities must comply with in relation to the use or display of the digital ID trustmark.

5.5 The digital ID trustmark may be used by any accredited entity with public-facing accredited services and is not restricted to use only by accredited entities participating in the AGDIS.

5.6 Subrule 5.1(2) provides that, for the purposes of paragraph 168(1)(b) of the Digital ID Act, this Chapter also specifies the digital ID trustmark that may be used by an entity specified in rule 5.4 (defined in this subrule to be an ***authorised entity***, and listed in subrule 5.4(2)), as well as the conditions in relation to the use or display of that digital ID trustmark.

5.7 A Note to subrule 5.1(2) explains that there are provisions in the Digital ID Act which impose civil penalties for non-compliance with the Digital ID Act and the Rules in the use of the trustmark. Subsection 118(2) of the Digital ID Act creates a civil penalty provision for the unauthorised use of the Digital ID trustmark, with a civil penalty of up to 1,000 penalty units. Section 119 of the Digital ID Act creates a civil penalty provision if an entity fails to comply with conditions specified in the Rules in relation to the use or display of a digital ID trustmark. These provisions are enforceable by the Digital ID Regulator under the *Regulatory Powers (Standard Provisions) Act 2014*, which sets out relevant evidentiary requirements.

5.8 Subrule 5.1(3) provides that this Chapter does not affect or limit rights or remedies arising under other laws in respect of a digital ID trustmark or an element of a digital ID trustmark. This ensures that the operation of all other laws is unaffected by this Chapter. For example, any rights or remedies that may arise in relation to intellectual property under the *Trade Marks Act 1995*, *Designs Act 2003*, *Copyright Act 1968* or the *Competition and Consumer Act 2010*.

5.9 Subrule 5.1(4) provides that the term ***authorised entity*** has the meaning given by subrule 5.1(2) and the term ***Digital ID Accreditation Trustmark*** has the meaning set out in subsequent rule 5.2.

**Rule 5.2 Digital ID trustmark**

5.10 This rule provides that the digital ID trustmark set out in item 1 of Schedule 1 may be used by an accredited entity and an authorised entity.

5.11 Importantly, this rule makes clear that use of the digital ID trustmark by accredited or authorised entities is optional, not mandatory.

**Rule 5.3 Use or display of digital ID trustmark—accredited entities**

5.12 Subrule 5.3(1) provides that rule 5.3 prescribes conditions and requirements that accredited entities must comply with when using or displaying the digital ID trustmark.

5.13 Where an accredited entity uses or displays the digital ID trustmark, the accredited entity must take reasonable steps to make clear to the user of an accredited service when they are interacting with a part of a service that is accredited, and when they are not. For example, placement of the trustmark at the top of a list of every service an entity provides (including non-accredited services) would not be permitted. The use or display of the digital ID trustmark must be specifically in relation to the accredited services provided by the entity.

5.14 Subrule 5.3(2) provides that the Digital ID Accreditation Trustmark may only be used or displayed by an accredited IXP in 2 circumstances.

5.15 First, the IXP may use or display the mark on public-facing accredited services of the IXP. This could include displaying the digital ID trustmark next to the login option on an identity provider's website, indicating that you can log into the exchange to receive the accredited services displayed with the trustmark.

5.16 Secondly, the IXP may use or display the mark on any documents containing public-facing information related to accredited services concerning:

- the accredited services of the IXP itself (for example, a brochure or webpage of a bank providing accredited services); or
- the accredited services of another accredited entity operating within the same digital ID system as the accredited services of an IXP.

5.17 An Example under subparagraph 5.3(2)(b)(ii) relevantly provides that this rule would allow an IXP to publish a list of its service providers (for example, on a webpage). That list of services could include both accredited and unaccredited services, and the Digital ID Accreditation Trustmark could be used to distinguish between the various services.

5.18 Rule 1.4 provides for the definition of an ***IXP***, ***public-facing accredited services*** and ***public-facing information related to accredited services***.

5.19 Subrule 5.3(3) sets out requirements for accredited entities when using or displaying the digital ID trustmark. They include:

- use and display a hyperlink to the Digital ID Accredited Entities Register (established and maintained by the Digital ID Regulator under section 120 of the Digital ID Act) near the digital ID trustmark;

- for documents which are, or can be, printed in hard-copy – the accredited entity must use and display the internet address (uniform resource locator) of the Digital ID Accredited Entities Register near the digital ID trustmark; and
- where an accredited entity provides services other than accredited services, the entity must take reasonable steps to make clear which services are accredited and which are not.

5.20 The term ***document*** is defined in the *Acts Interpretation Act 1901* to mean any record of information. Examples of documents can include electronic documents (such as webpages or mobile applications) or printed documents.

5.21 Subrule 5.3(4) provides that if an entity has their accreditation suspended or revoked, the entity has 7 days to cease use or display of the digital ID trustmark.

**Rule 5.4 Use or display of digital ID trustmark – authorised entities**

5.22 Subrule 5.4(1) provides that rule 5.4 prescribes conditions in relation to the use or display of the digital ID trustmark by an authorised entity. The term condition is used within this rule in a general sense, and should not be confused with other types of conditions that may be placed on accredited entities or participating relying parties by the Rules or the Digital ID Regulator.

5.23 Subrule 5.4(2) prescribes the Digital ID Regulator, the System Administrator, the Information Commissioner, and the Secretary of the Department of Finance as authorised entities.

5.24 Subrule 5.4(3) provides that an authorised entity may only use or display the digital ID trustmark for the purpose of the performance of functions under or in relation to the Digital ID Act, education in relation to 'this Act', and promotion of the objects of 'this Act'. 'This Act' is defined in section 9 of the Digital ID Act.

5.25 The purpose of rule 5.4 is to permit government entities with roles under, or in relation to, the Digital ID legislative framework, to use or display the digital ID trustmark in order to fulfil their functions and build awareness and trust in relation to the AGDIS.

# Chapter 6—Record-keeping

### Rule 6.1 Application of this Chapter

6.1 Subrule 6.1(1) provides that for the purposes of subsection 135(3) of the Digital ID Act, an entity specified in subrule 6.1(2) must keep records of the kind, for the period, and in the manner prescribed by this Chapter of the Rules.

6.2 Subrule 6.1(2) provides that, subject to subrule (3), this Chapter applies to entities holding approval to participate in the AGDIS, as well as entities whose approval to participate in the AGDIS is suspended, or has been revoked.

6.3 Subrule 6.1(3) clarifies that this Chapter does not apply to a relying party.

6.4 Subrule 6.1(4) makes clear that if an entity's accreditation is suspended or revoked by the Digital ID Regulator, this Chapter of the Rules will continue to apply to that entity even after its accreditation has been suspended or revoked.

### Rule 6.2 Record keeping requirements

6.5 Subrule 6.2(1) provides that an entity must keep a prescribed record for whichever of the following periods ends later:

- the period of 3 years that starts on the day the record was created; or
- 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.

6.6 The definition of ***prescribed record*** is set out in subrule 6.2(3). A prescribed record of an entity means a record that is a log that an entity is required to keep under subrule 4.20(7) of the Accreditation Rules, where that record also contains personal information. The definition of personal information is set out in section 9 of the Digital ID Act.

6.7 Subrule 6.2(2) provides that an entity must not destroy or de-identify information contained within a prescribed record in the circumstances set out in that provision. The prohibition applies where:

- the information is personal information (that is not biometric information) obtained by the entity in the course of providing its accredited services;
- the entity is required or authorised to retain that information; and
- the information relates to a current or anticipated legal or dispute resolution proceedings, or a current compliance or enforcement investigations under 'this Act' (defined in section 9 of the Digital ID Act), to which the entity is a party.

6.8 As provided for in subrule 6.1(3), these record-keeping requirements apply regardless of whether the entity has ceased to be accredited within the time period specified in 6.2(1), which is 3 years after the relevant event.

6.9 Subrule 6.2(2) is intended to cover situations where, for example, due to actions by the Digital ID Regulator, the accredited entity holds information which is

related to anticipated legal proceedings. In that situation, the accredited entity would be prohibited from destroying records related to the anticipated legal proceedings under this provision. As provided for in subrule 6.1(3), this record-keeping requirement will apply regardless of whether the entity has ceased to be accredited within the time period specified in subrule 6.2(1).

6.10 In complying with the record keeping requirements of the Rules, the accredited entity must also continue to meet its privacy obligations in the Accreditation Rules, including the data minimisation principle. Additionally, the accredited entity must comply with the *Privacy Act 1988* and the additional privacy safeguards within the Digital ID Act.

6.11 Accredited entities participating in the AGDIS must also continue to comply with section 136 of the Digital ID Act, which deals with destruction and de-identification of personal information in the possession or control of accredited entities, where they are no longer required to keep that information.

6.12 Civil penalties associated with record-keeping requirements in the Rules are provided for under subsections 135(3) and 136(2) of the Digital ID Act, which will allow the Digital ID Regulator to take enforcement action for non-compliance with these record keeping requirements.

# Schedule 1—Digital ID trustmark

Schedule 1 specifies the digital ID trustmark for use by an accredited entity for the purpose of subrule 5.2.

Chapter 5 of the Rules provide for the use and display of the digital ID trustmark which is the image below.

**ATTACHMENT B**

# Statement of Compatibility with Human Rights

*This statement is prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011*

***Digital ID Rules 2024***

The *Digital ID Rules 2024* (the Rules) are compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011.*

## Overview of the Rules

The Rules set out the requirements for accredited entities and relying parties to participate in the Australian Government Digital ID System (the AGDIS) on commencement of the *Digital ID Act 2024* (the Digital ID Act) and provides for:

- fit and proper person considerations relevant to accreditation and participating in the AGDIS;
- requirements for participating in the AGDIS;
- record keeping obligations for certain entities;
- arrangements relating to the notification and management of cyber security and digital ID fraud incidents that have occurred in relation to the AGDIS, including information sharing powers for the System Administrator; and
- obligations and conditions on accredited entities regarding the use or display of the specified image of Australia's Digital ID Accreditation Trustmark (the digital ID trustmark), as provided for under Chapter 8 of the Digital ID Act.

## Human rights implications

The principal human right that the Rules engage is the prohibition from arbitrary or unlawful interference with privacy contained in Article 17 of the International Covenant on Civil and Political Rights (ICCPR), and also referred to in Article 16 of the Convention on the Rights of the Child (CROC) and Article 22 of the Convention on the Rights of Persons with Disabilities (CRPD).

## PROTECTION FROM ARBITRARY OR UNLAWFUL INTERFERENCE WITH PRIVACY

Article 17 of the ICCPR prohibits arbitrary or unlawful interference with privacy. It states that:

- *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*

- *Everyone has the right to the protection of the law against such interference or attacks.*

Article 16 of the CROC, and Article 22 of the CRPD contain similar rights.

**MEASURES TO PROTECT FROM ARBITRARY OR UNLAWFUL INTERFERENCE WITH PRIVACY**

The Digital ID Act and the Rules aim to enhance the privacy of individuals who use digital IDs to access online services provided by entities participating within the AGDIS (referred to as relying parties). The Digital ID Act governs the collection, use, and disclosure of personal information used in digital ID services as well as the obligations of digital ID providers and users, including privacy obligations. These regulatory arrangements also provide a framework for oversight, accountability, and redress for individuals for breaches or misuse of their digital ID information including privacy breaches and misuse of their personal information.

The Rules promote the right to protection from arbitrary or unlawful interference with privacy by supporting the operation of the Digital ID Act by:

- Prescribing requirements for entities seeking approval from the Digital ID Regulator to participate in the AGDIS. For example, relying parties must conduct a risk assessment which identifies and manages cyber security or fraud incidents, and must have cyber security and fraud management plans in place to deal with such incidents. Entities applying to participate in the AGDIS must also have effective written procedures in place to notify the System Administrator of any actual or proposed change, outage or downtime in relation to their IT system that will, or could reasonably be expected to, have a material effect on the operation of the AGDIS.
- Requiring the Digital ID Regulator to consider whether an entity seeking approval to participate in the AGDIS has a background of privacy non-compliance (for example, if a privacy determination under the *Privacy Act 1988* has been made against the entity), should the Digital ID Regulator choose to consider the fit and proper person test at Chapter 2.
- Requiring accredited entities to notify the Digital ID Regulator if the entity proposes to use an IT system to provide or receive services within a different digital ID system. This enhances privacy as it enables the Digital ID Regulator to understand the information flows and interactions between the systems.
- Allowing the System Administrator to disclose information relating to cyber security and fraud incidents to the Digital ID Regulator or Minister to perform their functions or exercise their powers in order to protect the security, integrity or performance of the AGDIS.
- Setting out requirements on use and display of the digital ID trustmark in Chapter 5. The trustmark will indicate to prospective digital ID users that an accredited entity has met the pre-requisite standard of privacy protections and is subject to the additional privacy safeguards in the Digital ID Act.

In addition to the Rules, accredited entities who hold approval to participate in the AGDIS are also required to meet the privacy obligations under the Digital ID Act and the Accreditation Rules, which includes the data minimisation principle that limits the amount

of personal information that is collected and disclosed by accredited entities in providing digital ID services.

The Rules require entities to keep records of transaction and event information related to the use of digital IDs in the AGDIS. These records are designed to assist the Digital ID Regulator, and where applicable the Information Commissioner, to conduct investigations and compliance activities in relation to potential breaches of privacy and other safeguards in the Digital ID Act. These record keeping obligations work in conjunction with privacy-enhancing obligations in the Digital ID Act and the Accreditation Rules.

Despite engaging Article 17 of the ICCPR, these Rules promote the growth of, and trust in, digital ID services throughout the economy. The impacts on an individual are not arbitrary nor unlawful, and are reasonable and proportionate to give effect the objectives of the Digital ID Act.

The possible impacts on privacy enhance the protections for individuals in the Digital ID Act.

**Conclusion**

The Rules are compatible with human rights because they promote the protection of human rights and, to the extent that they may limit human rights, those limitations are reasonable, necessary and proportionate.

**Senator the Hon Katy Gallagher, Minister for Finance**