accc.gov.au

The Australian Government Digital ID System (AGDIS) Redress Framework

Guidance for entities: Requirements for the publication of incident and complaints management policies

Version 1.1 – September 2026

This fact sheet outlines the requirements for the publication of incident and complaints policies by approved Identity Service Providers (**ISPs**) and Attribute Service Providers (**ASPs**) participating in the Australian Government Digital ID System (**AGDIS**). In particular, it provides guidance on the requirements in rule 4A.8 of the *Digital ID Rules 2024* (**the Digital ID Rules**) on the development and publication of policies relating to complaints by individuals about cyber security incidents and digital ID fraud incidents.

ISPs and ASPs have a range of obligations under the AGDIS Redress Framework. This guidance focuses on the obligations relating to the policies that an ISP or ASP whose approval is not suspended or revoked is required to have published. Meeting this obligation is necessary to comply with the requirements of the AGDIS Redress Framework.

In addition to the obligations outlined in this factsheet, entities should also familiarise themselves with the requirements of rules 4A.2 and 4A.5 of the Digital ID Rules. These rules require entities to make reasonable attempts to notify each affected individual of digital ID fraud and cyber security incidents, and to provide information, support and assistance to affected individuals. The requirement applies to incidents involving digital IDs used in accredited services within the AGDIS.

Entities should also familiarise themselves with the Voluntariness obligation. The *Voluntariness obligations in the AGDIS* factsheet explains the requirement and includes practical examples and recommendations to support compliance.

This guidance is intended to complement the legislation by providing context and practical explanations. It should be read in conjunction with additional guidance for participants in the AGDIS that has been developed by the Australian Competition and Consumer Commission (**ACCC**) and is available on the Digital ID System website.

This guidance provides general information only and does not constitute legal advice. Organisations should seek independent professional advice to understand their obligations under the *Digital ID Act 2024* (**the Act**).

Throughout this factsheet, "entities" refers to approved ISPs and ASPs whose AGDIS approval remains **active** and **valid** (that is, it has not been suspended or revoked). "Digital ID incidents" refers to cyber security incidents and digital ID fraud incidents that occur or are reasonably suspected of having occurred.

Why have an AGDIS Redress Framework?

An AGDIS Redress Framework has been developed to support consumers and help resolve issues arising from digital ID fraud and cyber security incidents involving digital IDs used in accredited services within the AGDIS.

From identification to resolution: Developing and publishing cyber security incident and digital ID fraud response policies

There are 2 key obligations under the AGDIS Redress rules relating to the development and publishing of policies for the identification, management and resolution of Digital ID incidents, and for complaints made by individuals regarding Digital ID incidents. These obligations are set out in Part 5 of Chapter 4A of the Digital ID Rules.

The first obligation requires entities to develop and publish policies for the identification, management and resolution of Digital ID incidents.

The second obligation requires entities to develop and publish policies relating to complaints by individuals around digital ID incidents. The obligation is outlined in rule 4A.8 of the Digital ID Rules and is the focus of this guidance.

Entities should also familiarise themselves with rule 4.49 of the *Digital ID Accreditation Rules 2024* and understand their accessibility obligations. This includes presenting public-facing information about their accredited services in a clear, simple, and easy to understand way, and making that information available in accessible formats.

Do entities need a separate complaints policy for digital ID incidents?

Entities do not need to establish a separate complaints policy for digital ID incidents. They can use an existing complaints policy, provided it clearly covers digital ID fraud and cyber security incidents and prominently explains how individuals can make a complaint about these incidents.

This will help users quickly identify where to go and how to raise a complaint relating to digital ID fraud and cyber security incidents.

Entities must also ensure their complaints policy is easy for people to find, access and understand.

What *must* a complaints policy include?

An entity must:

- Publicly make available a complaints policy covering Digital ID incidents that occur or are reasonably suspected of having occurred.
- Include the following information in the policy:
  - how individuals can make a complaint to the entity, including relevant contact details; which may include (but not be limited to) a telephone number, email address or a chat function
  - procedures for dealing with complaints (including how complaints will be investigated) and a simple explanation of these procedures
  - the expected timeframe for resolving complaints.

In addition to the mandatory requirements outlined above, a well-designed complaints policy should also include the following best practice principles.

A well-designed complaints policy should include:

- Clear information about the available complaint channels, including:
  - the hours during which the complaint channels are available, for example Monday to Friday, 8:00am to 6:00pm
  - allowing complaints to be submitted easily and monitored regularly to support timely review and further investigation, where required.
- Information about the possible outcomes of the complaints process, including remedies, actions or responses that may be available to resolve a complaint, and any limitations on those outcomes.
- Details of review and escalation pathways, including the steps available if a complainant is dissatisfied with an outcome or does not receive a timely response.
- Accessible communication options for individuals who may have difficulty hearing or speaking on the phone.
- Language support for non-English speakers, including interpreting services where appropriate.

Making it easy to make a complaint: good and poor practice examples

Good practice means making it easy for people to understand the complaints policy and lodge a complaint without having to search extensively or overcome unnecessary barriers.

Good practice examples

- ✓ The website includes a clearly labelled "make a complaint" option that is prominent and accessible from the homepage.
- ✓ The complaints policy is written in plain language, is easy to understand, and considers the needs of vulnerable people.
- ✓ Reasonable steps are taken to ensure the information is available in multiple accessible formats.
- ✓ The complaints policy includes a dedicated email address or other contact point specifically for complaints.
- ✓ The policy links directly to an online complaint form rather than requiring users to navigate multiple pages.
- ✓ If using an AI chat function, ensuring it can recognise and accept complaints directly, or direct users to the appropriate complaints channel, without requiring them to repeatedly rephrase the issue.
- ✓ Where a telephone contact number is provided, a free international contact option should also be available for people calling from overseas.
- ✓ The entity promptly acknowledges receipt of the complaint.
- ✓ Clear information about expected response timeframes and confirmation that complaints channels are monitored regularly.
- ✓ Clear information about how complainants can check the status of their complaint.

Good practice Scenario

Alex wants to raise a complaint regarding a cyber security incident. On the entity's website, the complaints page is easy to find, clearly explains how to make a complaint, what information is needed, expected response timeframes, and what will happen next.

Alex submits the complaint online and receives confirmation of receipt, including a reference number and details of who will manage the complaint. The website also provides simple details on how the entity will resolve incidents, including the steps it will take. The organisation provides updates within the stated timeframe and communicates the outcome clearly, including any options for further review if required.

Alex feels the process was accessible, fair, and transparent.

Poor practice examples

- × The complaints policy uses complex language and does not adequately consider the accessibility and support needs of vulnerable users.
- × The complaints policy refers users to a generic "Contact us" page with no clear way to lodge a complaint.
- × The only available contact channel is an AI chatbox that does not recognise complaints or automatically redirects users through multiple menus.
- × Users are unnecessarily required to log in or create an account before they can submit a complaint.
- × The website only provides a webform and no alternate contact method.
- × Complaints emails are sent to an address that is not regularly monitored.
- × Users are required to navigate complex decision tree or select misleading and confusing categories before reaching a complaints form.

Poor practice Scenario

Alex wants to raise a complaint regarding a cyber security issue. On the entity's website, Alex is required to navigate through several "contact us" pages and interact numerous times with an AI chatbox before a complaints form is revealed. No email address or other contact information is provided, and Alex is not notified if the form was successfully submitted or how long it will take for the complaint to be looked at or attempted to be resolved. When Alex searches for information on the website about what to expect next, no relevant information is available.

Additional measures to support a good AGDIS Redress complaints policy

In addition to publishing a clear and accessible complaints policy, entities should also implement broader systems and practices that support effective complaints management.

These include:

- clear internal complaint handling procedures, including timeframes based on the urgency of the complaint
- clearly defined roles and responsibilities for managing complaints
- relevant staff training, support and guidance
- regular review of complaints policies and procedures to support continuous improvement
- effective tracking of complaints from initial receipt through to resolution or final decision
- clear processes for keeping complainants informed about the status of their complaint
- promoting an organisational culture that values effective complaint management
- processes for recording, tracking and reporting on complaints.

For more information on all the AGDIS Redress obligations, see Chapter 4A of the Digital ID Rules

ACCC 09/26_26-69 www.accc.gov.au