Australian Government

Australia's
Digital ID System

November 2024

AGDIS System Administrator Operational Handbook

System Administrator
Australian Government Digital ID System (AGDIS)

digitalidsystem.gov.au

Contents

IT system incidents

Restoring operations, services, and functions as quickly as possible is critical. This includes ensuring we minimise any impact on Australian Government Digital ID System (AGDIS) users.

Contact details and when to contact

Contact the System Administrator through the purpose built, secure, online portal known as the AGDIS Administrator Portal (the Administrator Portal).

Or email the System Administrator at AGDIS.Administrator@servicesaustralia.gov.au.

Incidents	
P1 incident – Critical **Notify within 30 minutes via the Administrator Portal or via email**	**Accredited Entity's service is degraded** Impacts include increased vulnerability for intrusion, abuse or fraud. Major impact to Participating Relying Party services, compromised data security or user privacy, or serious reputational impact.
P2 incident – High **Notify within 30 minutes via the Administrator Portal or via email**	**Accredited Entity's service not working as intended** Impacts include serious disruption to Participating Relying Party services, non-compliance with the Act or Rules, or risk of serious reputational risk impact.
P3 incident – Moderate **Notify within 24 hours via the Administrator Portal or via email**	**Non-critical degradation of Accredited Entity's service** Impacts include affecting a small number of users (less than 5%).
P4 incident – Low **Notify within 48 hours via the Administrator Portal or via email**	**Accredited Entity's Service experiencing a minor fault or component failure** Does not affect service availability and workarounds can be implemented. Includes all testing (non-production) environments where service availability is more than 25%

What to tell the System Administrator:

- **Entity details** (name and contact details)
- **Description** of incident
- **Impacts** (is this an outage? what systems are affected?)
- **Actions** (what message have been sent, what investigations are occurring?)
- **Incident number**
- **Time** incident started
- **Priority** of incident
- **Expected resolution time** (if known)
- **Time of next update** to the System Administrator

Fraud or cyber security?

For fraud or cyber security incidents, please also read the following sections of this Handbook:

Section 5.4 Fraud management and incident response for participating entities

Section 5.5 Cyber security management and incident response for participating entities

For further details about IT system incidents, refer to **Section 5.1** of this Handbook.

1 Introduction

1.1 Using this Handbook

This Handbook is for all entities participating in the AGDIS and describes how participating entities work with each other and the System Administrator.

> **Entity or Participating Entity** refers to an **Accredited Entity** (i.e. an accredited Attribute Service Provider, Identity Exchange Provider and Identity Service Provider) or a **Participating Relying Party** that operates within the AGDIS.

The relevant Digital ID legislation can be found at https://www.legislation.gov.au/:

- *Digital ID Act 2024* (the Act)
- *Digital ID Rules 2024* (the Rules)
- *Digital ID (AGDIS) Data Standards 2024* (the AGDIS Data Standards)
- *Digital ID Accreditation Rules 2024* (the Accreditation Rules)
- *Digital ID Accreditation Data Standards 2024* (the Accreditation Data Standards)
- *Digital ID Transitional and Consequential Provisions Act 2024* (the Transitional Act)
- *Digital ID Transitional and Consequential Provisions Rules 2024* (the Transitional Rules).

Note: this Handbook does not replace the requirement for participating entities to have a full understanding of the Digital ID legislation. Participating entities must also ensure they are familiar with any guidance or other information prepared by the Digital ID Regulator (represented by the Australian Competition and Consumer Commission, or ACCC), the Office of the Australian Information Commissioner (OAIC) and the Data Standards Chair.

1.2 Role of the System Administrator

The System Administrator is responsible for protecting the integrity and performance of the AGDIS. Section 95 of the Act defines the specific functions of the System Administrator:

- to provide assistance to entities participating in the AGDIS, including in relation to connecting to, and dealing with incidents involving, the system;
- to facilitate and monitor the use of the AGDIS for testing purposes, in accordance with any requirements specified in the Rules;
- to monitor and manage the availability of the AGDIS, including by coordinating system changes and outages and by ensuring that changes made by entities that are participating in the AGDIS do not adversely affect the system as a whole;
- to identify and manage operational risks relating to the performance and integrity of the AGDIS;
- to manage digital ID fraud incidents and cyber security incidents involving entities participating in the AGDIS;
- to advise the following, either on its own initiative or on request, on matters relating to the operation of the AGDIS:
  - the Minister;
  - the Digital ID Regulator;
  - the Digital ID Data Standards Chair;
- to advise the Information Commissioner, either on its own initiative or on request, on privacy matters that relate to the AGDIS;
- to report to the Minister, on request, on the performance of the System Administrator's functions, and the exercise of the System Administrator's powers, under this Act;
- to share information with the following, to assist them to exercise their powers

or perform their functions under this Act:

  - the Minister;
  - the Digital ID Regulator;
  - the Digital ID Data Standards Chair;
  - the Information Commissioner;
- such other functions as are conferred on the System Administrator by this Act or any other law of the Commonwealth;
- to do anything that is incidental or conducive to the performance of any of the above functions.

1.3 Powers of the System Administrator

Section 96 of the Act gives the System Administrator the power to do all things necessary or convenient to be done for, or in connection with, the performance of the System Administrator's functions under the Act.

Section 130 of the Act gives the System Administrator the power to give written directions to entities to protect the integrity or performance of the AGDIS.

Section 134 of the Act gives the System Administrator the power to request, by written notice, any information or documents relevant to the operation of the AGDIS, within a specified timeframe. The timeframe must not be less than 28 days after the written notice is given.

1.4 When to contact the System Administrator

The System Administrator uses the Administrator Portal to manage fraud and cyber incidents, change and release and IT system incidents. All communication, including initial notification to the System Administrator, can be done via the Administrator Portal.

Users of the Administrator Portal must be registered. Users must be located within Australia as offshore users will not be granted access to the Administrator Portal.

Who to notify	When to notify
System Administrator team Online via the Administrator Portal.	**When planning a system change** If a participating entity intends to release a notifiable change to their service. **When a digital ID fraud or a cyber security incident is detected** If a participating entity becomes aware of, or suspects to have occurred, a reportable digital ID fraud or a cyber security incident **When an IT system incident is identified** If an **Accredited Entity** identifies a system incident which has led to, or could lead to, a defect, disruption, or degradation of their service. This includes unplanned outages of critical non-production systems.
System Administrator team Email via AGDIS.Administrator@servicesaustralia.gov.au	**When needing to change contact information** If a participating entity needs to update their contact information due to a user leaving the program, or a new user being added. **Note:** entities will be able to update their team information using the Administrator Portal in the future via 'Manage My Teams'.

1.5 Governance

Delivering Digital ID is the responsibility of many government entities. Each entity has responsibility for certain deliverables, and each contributes to the program's direction through governance mechanisms.

The structure includes 4 key governance areas: oversight, portfolio, program and teams.

The 2 key governance bodies are the Digital ID Steering Committee and Program Board, underpinned by a series of working groups. All working groups report to meeting owners and the respective agency executives. Reporting and escalating to the Program Board occurs as required.

The Act splits responsibility for the oversight and daily operation of the AGDIS into 2 independent authorities:

- the Digital ID Regulator is the ACCC, as per sections 89-92 of the Act, and
- the Digital ID System Administrator is the Chief Executive Centrelink, within the meaning of the *Human Services (Centrelink) Act 1997*, as per sections 93-97 of the Act.

1.6 Freedom of Information

The role of the System Administrator is separate to the role of the Digital ID Regulator. As such, requests to the System Administrator under the *Freedom of Information Act 1982* are managed through the existing processes of Services Australia. Requests will be transferred between the System Administrator and the Digital ID Regulator where required.

For more information on Services Australia's processes, refer to servicesaustralia.gov.au/freedom-information.

1.7 Participating entity's contact information

The processes within this Handbook uphold the principles of a privacy enhancing system, by limiting the information shared about individual users when interacting with the System Administrator and other entities.

When providing personal information, participating entities must ensure the disclosure is in line with the AGDIS System Administrator Data Sharing Principles, meets the *Privacy Act 1988* (the Privacy Act) and the Australian Privacy Principles (the APPs).

This does not limit or replace the privacy requirements for entities participating in the AGDIS, as outlined in sections 32-56 of the Act.

For more information, contact AGDIS.Administrator@servicesaustralia.gov.au.

2 Reviews and complaints for entities

2.1 Compliance reviews

To ensure the integrity of the AGDIS, compliance reviews are performed. These reviews may be triggered by complaints, incidents (such as system outages and fraud or cyber security issues), notifications of significant changes, monitoring processes, or direction by the System Administrator.

Compliance and enforcement activities may be conducted by the Digital ID Regulator under sections 122-129 of the Act. Where the System Administrator identifies potential non-compliance, the matter may be referred to the Digital ID Regulator as appropriate. For more information on the System Administrator's referral process, please refer to the System Administrator's Compliance Referral and Reporting Strategy on the digitalidsystem.gov.au website.

2.2 Reviews of decisions

Reviewable decisions

The System Administrator has the power to give directions to entities in accordance with section 130 of the Act:

1. The System Administrator may give a written direction to the following entities if the System Administrator considers it necessary to do so to protect the integrity or performance of the AGDIS:
   a. entities that hold an approval to participate in the AGDIS;
   b. entities whose approval to participate in the AGDIS is suspended.
2. Without limiting subsection (1), the System Administrator may give a written direction to do one or more of the following:
   a. take or not take specified action in relation to the performance of the AGDIS;
   b. conduct a fraud assessment in relation to a specified matter and provide a copy of the report to the System Administrator in relation to the assessment;
   c. conduct a security assessment in relation to a specified matter and provide a copy of the report to the System Administrator in relation to the assessment;
   d. an act or thing specified by the Rules.
3. If Accreditation Rules made for the purposes of s 28 of the Act prescribe requirements in relation to the conduct of an assessment mentioned in subsection (2), the assessment must comply with the requirements.
4. The direction must:
   a. be in writing; and
   b. specify the reason for direction
5. An entity must comply with a direction given under subsection (1). Failure to do so may result in a civil penalty of 1,000 penalty units.

> **Internal review** – if an entity is unhappy with a decision made by the System Administrator under section 130 of the Act, it may request an *internal review* of the decision.
>
> **External review** – if an entity is unhappy with an internal review decision or a decision made personally by the Chief Executive Centrelink, it may request an *external review* of the decision.

Internal reviews of decisions

An entity affected by a decision made by a delegate of the System Administrator, under section 130 of the Act, can apply for a review (an internal review) if they disagree with the decision. This application must be made in writing and emailed to AGDIS.Administrator@servicesaustralia.gov.au.

In accordance with section 138 of the Act, an application for a review of a decision should be made within 28 days of the entity being notified of the original decision.

In accordance with section 139 of the Act, within 90 days of receiving an application under section 138 for a review of a decision, an internal review will be completed by a delegated officer of the System Administrator.

The internal review decision-maker will:

- review the relevant information and legislative framework
- arrange for additional assessments if required, and
- make a new decision, which affirms, varies or revokes the original decision.

The delegated officer will give the applicant a written statement of their reasons for the decision after a review is completed.

External reviews of decisions

Where an entity disagrees with:

- the outcome of a review (an internal review) by a delegated officer of the System Administrator, or
- a decision made personally by the Chief Executive Centrelink

they can request a review by the Administrative Review Tribunal in accordance with section 140 of the Act.

2.3 Complaints between entities

> **Note:** this section covers complaints between entities. For escalated user complaints and user support issues, see **Section 5.3** of this Handbook.

Where an entity identifies a system issue caused by another entity, the System Administrator should be notified in writing. Where matters of potential non-compliance have been identified, the System Administrator will assess for referral to the Digital ID Regulator.

The System Administrator will investigate the entity's complaint and take appropriate action, including referring for a compliance review if appropriate. During this process, the System Administrator may request information from entities or access information directly from the AGDIS.

The System Administrator aims to resolve complaints within 28 business days.

3 Onboarding

3.1 Onboarding with the System Administrator

The ACCC in their capacity as the Digital ID Regulator is responsible for approving participation in the AGDIS.

The System Administrator provides assistance with the onboarding process prior to an entity seeking approval from the Digital ID Regulator. We facilitate access to the testing environment and serve as the front door for support and matters that require co-ordination to join the AGDIS from other areas such as identity service providers and identity exchange providers. We aim to ensure your experience in joining the AGDIS is seamless.

An entity should register their interest in joining the AGDIS by submitting the webform hosted on the digitalidsystem.gov.au website.

Entities that are already participating in the AGDIS and wish to onboard additional services to existing connections, should first apply to the Digital ID Regulator. Once approved, the entity must follow the change enablement procedures as outlined in **Section 4.1 (Accredited Entities)** and **Section 4.2 (Participating Relying Parties)** of this Handbook to notify the System Administrator.

Entities that are already participating in the AGDIS, and wish to onboard new services with new connections, must first complete the required testing before seeking approval to participate. Entities register their interest by submitting the webform hosted on the digitalidsystem.gov.au website.

4 Operational Standards

Future service levels for participating entities

Service levels will be set in the future by the Digital ID Data Standards Chair (DSC), in accordance with section 80 of the Act.

The service levels will formalise expected measurable performance for participation in the AGDIS. Specific service level standards set in the future by the Digital ID DSC will be updated in this Handbook accordingly.

Operational Standards

In the absence of service levels, the System Administrator has set the below operational standards to ensure the performance and integrity of the AGDIS is maintained. These are in addition to the requirements listed in the legislation, for example notifications of fraud/cyber incidents.

4.1 Operational standards for Accredited Entities

Operational hours and availability standards

Service available	**24/7**
Target	**99.5%**

Accredited Entities will provide an uninterrupted service with a continuous stream of successful transactions.

Planned outages will be exempt from the target if the System Administrator has received at least 30 business days' notice and has approved the outage.

Reporting to the System Administrator: **Accredited Entities** will send the monthly system availability report in the first week of the next month.

The System Administrator will then develop the system-wide **monthly system availability report**, sent out by the 21st of the next month. This will include the service availability data for all **Accredited Entities**.

Monthly system availability report
Please use the template and include:

- **total hours and minutes** for the System Availability Calendar
- **total hours and minutes** for any planned outages impacting service availability from 5am to midnight, and
- **total hours and minutes** for any unplanned outages at any time.

If there were any unplanned outages, please provide the Administrator Portal reference number(s) in the Notes section of the template.

IT system incidents, unplanned outages and recovery time objectives (RTOs)

Administrator Portal available	**24/7**
Target for notifications	**95%**

Accredited Entities will notify the System Administrator via the Administrator Portal of all incidents and unplanned outages to their service (in both production and non-production).

Notification timeframes and recovery time objectives

Incident Priority		Notification Timeframes	Recovery Time Objectives (RTOs)
🟥	P1 – Critical	Notify **within 30 minutes** via the **Administrator Portal** or **email** (ensuring details are entered in the **Administrator Portal** within 24 hours originally notified by email)	P1 incidents resolved **within 4 hours**
🟧	P2 incident – High	Notify **within 30 minutes** via the **Administrator Portal** or **email** (ensuring details are entered in the **Administrator Portal** within 24 hours if originally notified by email)	P2 incidents resolved **within 24 hours**
🟨	P3 incident – Moderate	Notify **within 24 hours** via the **Administrator Portal**	P3 incidents resolved **within 7 days**
⬜	P4 incident – Low	Notify **within 48 hours** via the **Administrator Portal**	P4 incidents resolved **within 20 days**

These notification timeframes and RTOs are for:

- the initial reporting of an incident
- an **Accredited Entity's** response to a System Administrator notification (monitoring system detection)
- where an incident owner changes the incident priority, and
- IT system incidents only, not broader remedial efforts.

The incident owner must:

- keep the System Administrator informed of all investigation, mitigation and resolution activities (refer to **Section 5.1** of this Handbook for the expected frequency), and
- notify the System Administrator of incident resolution **within 30 minutes** via **the Administrator Portal** or **email**. If notifying by email, details must be entered into the Administrator Portal within 24 hours.

The System Administrator will:

- facilitate all incident communication to entities, and
- alert **Accredited Entities** where System Administrator monitoring detects their service is potentially down or degraded.

Change enablement notification operational standards

Accredited Entities must notify the System Administrator via the **Administrator Portal** of any changes or releases, including planned outages and system maintenance to their service (this also includes changes in the testing environment) within these timeframes:

Change Notification	Notification Timeframes
Initial change	No later than 5 business days after a participating entity becomes aware of a **planned** or **proposed** change where the change will, or could reasonably be expected to, have a material effect on the operation of the AGDIS via the **Administrator Portal**. **Note**: 'becomes aware' means where a participating entity: • first seeks internal approval for a **planned** change, or • is first notified internally of a proposed change (which may or may not eventuate).
Full details of change	30 calendar days prior to a planned change via the **Administrator Portal**. The System Administrator may require additional approvals where appropriate.
Confirmation of change proceeding	5 days prior to a scheduled release date via the **Administrator Portal**.
Post-release outcome	Within 4 days of the release date via the **Administrator Portal**.

4.2 Operational Standards for Participating Relying Parties

Change enablement notification operational standards

Participating Relying Parties must notify the System Administrator via the Administrator Portal of any changes or releases, including planned outages and system maintenance to their service (this also includes changes in the testing environment) within these timeframes:

Change Notification	Notification Timeframes
Initial change	No later than 5 business days after a participating entity becomes aware of a **planned** or **proposed** change where the change will, or could reasonably be expected to, have a material effect on the operation of the AGDIS via the **Administrator Portal**. **Note**: 'becomes aware' means where a participating entity: • first seeks internal approval for a **planned** change, or • is first notified internally of a **proposed** change (which may or may not eventuate).
Full details of change	30 calendar days prior to a planned change via the **Administrator Portal**. The System Administrator may require additional approvals where appropriate.
Confirmation of change proceeding	5 days prior to a scheduled release date via the **Administrator Portal**.
Post-release outcome	Within 4 days of the release date via the **Administrator Portal**.

4.3 Change enablement and release and deployment management

The System Administrator maintains the overarching change enablement practices, in collaboration with participating entities. This ensures changes are known by all impacted entities beforehand and allows them to manage the change impacts within their own business and ICT environments.

Change enablement (change management) is the process of following standardised procedures for efficient handling of changes to the services to minimise the risk and potential disruption to the service.

Release management is the process of managing, planning and scheduling the deployment of service changes through different environments.

Change impacts include ICT/system, policy, process, and people change management.

Standard change is pre-authorised, autonomous to an entity organisation, low risk and no impact to the other entities of the AGDIS.

Normal change is a medium risk and is not urgent or pre-approved. These are assessed for impacts to other parts of the AGDIS.

Major change is higher risk, significant impact to the AGDIS, requires coordination with other entities and may be part of a major release.

Emergency change is a change that needs to be implemented immediately (such as resolving a Major Incident). An emergency change may also be Standard, Normal or Major.

System Administrator responsibilities

The System Administrator is responsible for coordinating, overseeing, and providing assurance over changes and approved releases affecting the AGDIS where these changes could affect other entities or users. The System Administrator has responsibility, as the administratively independent body, to manage system-wide matters affecting stability, reliability, and integrity as well as overarching reporting and review requirements.

The procedures in this handbook support existing processes within entities. These standardised controls are agreed IT governance in the Act, the Rules, the Accreditation Rules and the Accreditation Data Standards. This is important because some changes and releases will impact other entities. This ensures:

- clear visibility of planned changes and outages in the AGDIS to allow impacted entities to schedule their own corresponding changes and prepare on-call teams
- coordination and better resource management over a release window where dependencies are prioritised and monitored
- mature performance communication and monitoring to enhance public and peer trust in the AGDIS.

The role of the System Administrator is not to assess or review a participating entity's change enablement, or release and deployment processes, or related activities undertaken in their own organisation. **Each entity is responsible for how they manage their respective change enablement and release and deployment practices.**

However, where a change or release (including planned maintenance activities) may have an impact on the performance, integration or availability of the AGDIS, the System Administrator will conduct:

- system-wide change governance
- change assessment and system-wide coordination
- coordination and facilitation of Virtual Change Advisory Board (VCAB) meetings
- coordination of change and release communications
- maintenance of a system-wide Change Register.

Examples of notifiable changes and releases

Here are examples of notifiable changes and releases, including major quarterly release cycles:

- An infrastructure change that could impact the performance, functionality or availability of a user's digital ID
- A change, or release of a change, to a **Participating Relying Party's** authentication configuration
- A change to a **Participating Relying Party's** Identity Proofing requirements or adding an additional approved service
- A change, or release of a change, to the entity service that requires a corresponding action by another entity
- A change, or release of a change, that will result in a total outage of the **Accredited Entity's** service
- A new entity is onboarding to the AGDIS
- A change to an **Accredited Entity** to rectify a problem, deliver new functionality or any other change, including where the service will be unavailable to users for a period of time.

Virtual Change Advisory Board (VCAB)

The VCAB is a vital function in the change enablement process. VCAB enables stakeholders to jointly assess and plan for the implementation of major system changes. All entities impacted by a specific change or release event will be identified by the System Administrator and invited to attend the VCAB. The VCAB will:

- review the effect of proposed Normal and Major (including Emergency) changes reported by entities to the System Administrator
- provide an opportunity for entities to ask questions to understand the proposed change
- evaluate the proposed change for risks to the AGDIS and identify mitigation
- ensure the proposed change is documented and well understood
- ensure the proposed release date is appropriate and doesn't conflict with other changes or operational activities
- determine the likelihood of unintended impacts to the AGDIS
- allow for Change Owners and impacted entities to make recommendations to reduce risk and minimise impact to the AGDIS.

You can request the VCAB Terms of Reference via email to AGDIS.Administrator@servicesaustralia.gov.au

5 Incidents, escalations and urgent matters

5.1 IT system incident management for Accredited Entities

> An **IT system incident** is an event that has, or could, lead to a disruption, interruption or degradation of the system's operations, services, or functions.
>
> The **incident owner** is the best-placed **Accredited Entity** to diagnose and resolve the issue. The incident owner leads all activities to resolve the incident and keeps the System Administrator informed.

This section covers the IT system incident management process for the AGDIS, including:

- notification
- communication, and
- resolution.

This Handbook details how the System Administrator supports the restoration of services as quickly as possible. For fraud and cyber incidents not affecting the availability of the AGDIS, **Accredited Entities** need to follow the sections of the Handbook:

- **Section 5.4** Fraud management and incident response
- **Section 5.5** Cyber security management and incident response.

IT system incident notification

Use the priority matrix below to determine the severity and priority of the IT system incident being reported. The priority will determine the notification timeframes and recovery time objectives.

IT system incident priority matrix

The priority of IT system incidents and how they are treated depends on the priority. This is based on both urgency (how quickly a resolution is needed) and impact (to business, to digital ID users, the AGDIS's reputation, and ministerial and legislative expectations). Impact to the AGDIS is considered, as well as impact to an individual entity. Thus, the priority determined by the System Administrator may be different to the view taken by **Accredited Entities**.

System availability will be largely determined using the Availability Monitoring Application. System availability will be verified with **Accredited Entitie**s wherever possible.

Circumstances which increase the impact severity may be considered and increase priority regardless of system availability. This could include sensitivities or considerations specific to a Participating Relying Party.

Availability for users	≤ 100%	≤ 95%	≤ 75%	≤ 25%
Participating entity service is degraded	4	3	2	1
Participating entity service is not working as intended	4	3	2	1
Participating entity service – critical non-production environment is degraded	4	4	4	3
Other factors that may increase priority				
Increased vulnerability for intrusion, abuse or fraud	1			
Legislative commitment or obligation, or ministerial deadline cannot be met	1			
Serious reputational damage to the System	1			
System processing or data causing compromised user privacy or safety	1			
High likelihood of serious non-compliance with accreditation requirements	1			
Apparent non-compliance with accreditation requirements	2			
Risk of serious reputational damage to the System	2			
Participating Relying Parties unable to deliver critical functions	2			

When an IT system incident is identified, the **Accredited Entity** responsible for the incident **must** notify the System Administrator via the **Administrator Portal**.

IT system incident notification timeframes

- **P1 (Critical)** incidents **within 30 minutes** via the Administrator Portal or email and provide updates every 30 minutes thereafter (if originally notifying via email, ensure details are entered into the Administrator Portal within 24 hours)
- **P2 (High)** incidents **within 30 minutes** via the Administrator Portal or phone between the hours of 8.00 am to 5.00 pm (AEST) and provide updates hourly thereafter (if originally notifying via email, ensure details are entered into the Administrator Portal within 24 hours)
- **P3 (Moderate)** incidents **within 24 hours** via the Administrator Portal and provide updates daily thereafter
- **P4 (Low)** incidents **within 48 hours** via the Administrator Portal and provide updates every 5 days thereafter.

If an incident changes severity or impact, the incident owner must update the System Administrator and use the appropriate timeframes.

When giving notification to the System Administrator the following information must be included:

- the Accredited Entity's name;
  - the contact details for the entity;
  - if the incident relates to an associated person of the entity—the name and contact details of the associated person;
  - a description of the incident;
  - the following details;
    - the date and time of the incident; and
    - the date on which the entity became aware of the incident.

Based on the information provided, together with information sourced from System Administrator monitoring and Participating Relying Parties, IT system incidents will be independently triaged to determine the owner and priority. This will determine the System Administrator's coordination activities, including communication. The incident owner is responsible for managing the IT system incident through to resolution. The owner is not always the Accredited Entity who reported the incident.

IT system incident communication

The System Administrator will facilitate SMS and email communication to impacted entities during the life cycle of an IT system incident, appropriate to the priority.

- **P1 – 2 hourly** communications, or whenever new information requires dissemination
- **P2 – 2 hourly** communications, or whenever new information requires dissemination
- **P3/4 –** will be discretionary

Note: the System Administrator will provide closure communications to all impacted entities.

IT system incident resolution

Priority levels and resolution targets

An incident will be assigned priority based on the priority matrix. Targets to resolve an IT system incident, as stated below, refer to service recovery and do not include broader remedial efforts.

Incident resolution targets and non-compliance referral ratings		
Priority	**Resolution performance target**	**Non-compliance referral rating**
P1 – Critical	Resolved within 4 hours	**1 – Very High**
P2 – High	Resolved within 24 hours	**2 – High**
P3 – Moderate	Resolved within 7 days	**3 – Medium**
P4 – Low	Resolved within 20 days	**4 – Low**

Prior to resolving an IT system incident, the System Administrator may contact impacted entities to complete a health check.

Accredited Entities: where an IT system incident has resulted in a possible, unintended breach of the legislation (such as a defect in the service) the entity should report this to the Digital ID Regulator. Any remediation changes to correct this breach should be registered through the Administrator Portal as per the usual change enablement process.

Where required, the System Administrator will direct an incident owner to conduct a Post-Incident Review (PIR) on the internal management of the issue.

The PIR provides an opportunity to identify and validate issues including initiation, communication and response. A PIR conducted by the incident owner will not examine the root cause or technical resolution action taken. If an affected entity would like a PIR to be conducted into the root cause of the incident, they should contact the System Administrator to make an assessment before they issue a direction.

Availability Monitoring Application

The Availability Monitoring Application is a tool that monitors stability and availability of the AGDIS, including each **Participating Relying Party** service.

Where the System Administrator has identified a potential issue with an **Accredited Entity** the tool will issue the responsible entity with an automated advice. The responsible **Accredited Entity** will then need to perform a health check, and:

- respond to the automated advice
- (if the IT system incident is not yet resolved) provide all mandatory incident information to the System Administrator (see **Section 5.1** of this Handbook), or
- (if the IT system incident is resolved) provide appropriate details as per the IT system incident management process above.

5.2 IT system incidents for Participating Relying Parties

Participating Relying Parties should assess an IT system incident to determine whether it has a material effect on the AGDIS as per Rule 3.4 (Item 2) of the Rules. If it is considered that it does have a material effect, the IT system incident **must** be reported as per **Section 5.1** of this Handbook.

If a Participating Relying Party identifies an IT system incident that relates to an Accredited Entity's service, they **may** report it at any time via the Administrator Portal.

> **User support issue** is a technical system issue or escalated service enquiry for an entity's service.
>
> **User complaint** is a user communicating dissatisfaction to an entity.

5.3 Escalated user support issues and complaints

This section supports participating entities to resolve escalated user support issues and complaints.

Participating entities are responsible for providing their users with technical support and managing complaints. Where an entity cannot resolve a user support issue or complaint because it relates to other services in the AGDIS, for example, the Identity Exchange or an Identity Service Provider, the participating entity can escalate to the System Administrator.

The System Administrator does not accept escalations or enquiries directly from end users. All escalations to the System Administrator must come through either:

- an entity service, or
- a third-party organisation such as an Ombudsman or Ministerial office.

Before referring an issue to the System Administrator, all entities should:

- ensure that the issue can't be resolved without escalation,
- explore all self-help options, including directing the user to existing resources such as information from the relevant entity, the digitalidsystem.gov.au website or other publicly available resources, and
- help the user identify the correct entity to provide support and give the user the entity contact information. If appropriate, conduct a warm hand-off to the entity.

Participating entities should escalate user support issues or complaints by completing the Escalated User Complaint form (please email AGDIS.Administrator@servicesaustralia.gov.au for a copy of this form) and then return it to AGDIS.Administrator@servicesaustralia.gov.au.

Note: entities will be able to escalate user support issues or complaints via the Administrator Portal in the future.

The System Administrator will aim to resolve the issue within 10 business days depending on the nature of the enquiry. Entities are expected to respond to escalation requests made by the System Administrator.

> For **digital ID fraud and cyber security user issues**, entities must comply with the following sections of this Handbook:
> - **Section 5.4** Fraud management and incident response
> - **Section 5.5** Cyber security management and incident response.
>
> Escalated user complaints regarding these topics may continue to follow the user complaints process in this section.

Entities are encouraged to use the digitalidsystem.gov.au website as a resource for internal stakeholders and for broader awareness of digital ID. Entities referencing information resources of other entities must first consult with that entity. For example, where a Participating Relying Party seeks to include a link to an Identity Service Provider's website.

Ensure user consent requirements are met when sharing personal information with the System Administrator

5.4 Fraud management and incident response for participating entities

Participating entities fraud control requirements

Accredited Entities must follow the fraud control requirements detailed in Part 4.2 of the Accreditation Rules. This includes having a fraud control plan as per Rule 4.31 of the Accreditation Rules.

Participating Relying Parties must follow the requirements in Chapter 3 of the Rules. This includes having a written digital ID fraud management plan as per Rule 3.3(2)(b).

Participating entities general obligations

Part 4.2 of the Rules sets out the requirements for **Accredited Entities** and **Participating Relying Parties** to report a digital ID fraud incident. Failure to adhere to the requirements may incur a civil penalty of 1,500 penalty units as per section 78 of the Act.

Pairwise identifiers for participating entities

The System Administrator has specifically designed the Administrator Portal web forms to limit the collection of personal information. In line with the AGDIS's privacy enhancing principles, when communicating with the System Administrator and with other entities, pairwise identifiers are used to specify users and user records. 2 types of pairwise identifiers are used:

- **IDP Link** – links the ID for an authenticated user at an Identity Service Provider (ISP) with the digital ID brokered by an Identity Exchange. This identifier is generated by the ISP.

- **RP Link –** links the digital ID brokered by an Identity Exchange to the service record at a **Participating Relying Party**. The Identity Exchange generates this identifier. An RP Link is unique for each user at each Participating Relying Party.

The System Administrator will never reveal pairwise identifiers to an entity, other than the one specifically associated with that entity's service.

Participating Relying Parties use of pairwise identifiers

As per Rule 3.4 (Item 3) of the Rules, all **Participating Relying Parties** must ensure they are able to search using a pairwise identifier to be able to identify a digital ID user. **Participating Relying Parties** must also ensure they are collecting and storing relevant pairwise identifiers (RP Links) in a readily retrievable way. This enables effective and accurate identification of a user record and communication with the System Administrator and other entities.

Pairwise IDs are issued in the payload from the Digital ID exchange for each authentication transaction. Pairwise IDs are unique to a user. They should be stored against an individual to enable entities to search for a user in their system and investigate or report fraud and cyber incidents.

What is digital ID fraud?

> A digital ID fraud incident is an act, event or circumstance connected to a participating entity that results in any of the following being compromised (confirmed or suspected) or rendered unreliable:
>
> - the digital ID of an individual
> - an attribute of an individual
> - a credential relating to an individual
> - a representation of an attribute or digital ID of an individual.

Digital ID fraud can be external or internal to participating entities. Examples can be found below.

Dishonestly registering or using a digital ID (generally external fraud), such as:

- a digital ID is established using stolen, fraudulently derived, fabricated or manipulated ID documents
- a digital ID credential is compromised by a third party
- multiple digital IDs are created for the same individual using different details and for dishonest purposes
- any of the above that could lead to dishonestly obtaining benefit or causing loss.

Employees within a participating entity:

- wrongfully using Commonwealth information or intellectual property of an ID provider or service
- undermining or manipulating fraud controls for an ID provider or service
- accessing, harvesting or exposing information from an ID provider or service
- otherwise exploiting or abusing a position of trust.

Role of the System Administrator

The System Administrator:

- helps transfer information between entities to investigate security, privacy and fraud incidents
- coordinates entity responses to incidents, ID theft, disaster recovery and other relevant issues
- undertakes inquiries and investigations in the AGDIS (which includes fraud)
- reports back to the entities on results of investigations.

Detecting fraud

Digital ID fraud can be detected throughout the digital ID lifecycle, including:

- during initial registration of an individual's digital ID
- through the consumption of a Participating Relying Party service
- by individuals, third-party organisations or law enforcement
- by an entity's fraud detection or reporting systems
- by the System Administrator, during a reportable fraud incident investigation.

Reporting suspected fraud incidents to the System Administrator

Participating entities must report suspected or confirmed digital ID fraud to the System Administrator. The System Administrator will undertake an investigation where required and notify all potentially impacted entities of the fraud.

As per Rule:

- 4.2 (4) of the Rules, participating entities must notify the System Administrator as soon as practicable after, and no later than one business day after, they become aware that an incident has occurred or reasonably suspects that an incident has occurred.
- 4.2 (5) of the Rules, this notification may be given orally, however if it is given orally, written notification must be given no later than 3 business days after the oral notification. Written notification is required via the Administrator Portal.

Where there are reasonable grounds to believe that there has been an eligible data breach (within the meaning of the Privacy Act), **Accredited Entities** that are APP entities, must give the Information Commissioner a statement that complies with section 26WK of the Privacy Act and give a copy of that statement to the Digital ID Regulator.

Where a fraud incident is impacting the availability of the AGDIS, the incident **must** be reported as outlined for an IT system incident in **Section 5.1** of this Handbook.

Reporting participating entity's investigation outcomes to the System Administrator

Where the System Administrator notifies an entity of suspected fraud, the entity **must** respond to the referral as per their Fraud Management Plan (**Participating Relying Parties**) or Fraud Control Plan (**Accredited Entities**).

Entities are required to acknowledge receipt of an Information Disclosure form sent by the System Administrator within 5 business days via the Administrator Portal.

Once an entity finishes an investigation (or when the facts are known), they must notify the System Administrator of the outcome.

The term 'investigation' in this Handbook refers to various types of reviews and does not necessarily mean a formal or criminal investigation.

Scenarios for reporting digital ID fraud incidents

The following scenarios show types of digital ID fraud events that need to be reported:

Scenario 1	**Third party data breach, ID information exposed, information used to create fraudulent digital IDs**
Details	A third-party data breach is reported to an Identity Service Provider (ISP). The breach involves exposure of ID document information. A check of ISP records confirms digital IDs were created with the exposed ID information. There are reasonable grounds to suspect the digital IDs may be fraudulent.
ISP must **immediately**	• follow their fraud management process • prevent the ongoing use of the suspicious digital IDs • notify the System Administrator (and submit a Request for Information if needed) • make all reasonable attempts to let impacted individuals know and help them recover their ID and remediate impacted services.
System Administrator **will**	• assess the notification and undertake an investigation where needed to identify all Participating Relying Party services that may have consumed the digital IDs • notify each of the Participating Relying Parties.
Participating Relying Parties **must**	• follow their fraud management process • where impacted, make all reasonable attempts to let impacted individuals know and help them to recover their ID and remediate impacted services • notify the System Administrator of the outcome.
Scenario 2	Criminal syndicate using Participating Relying Party services for fraud
Details	A Participating Relying Party receives a tip-off from law enforcement about a criminal syndicate using their services for fraud. Analysis identifies suspected fraud activities using digital IDs. There are reasonable grounds to suspect the digital IDs may be fraudulent.
Participating Relying Party must **immediately**	• follow their fraud management process • prevent the ongoing use of the suspicious digital IDs • notify the System Administrator (and submit a Request for Information if needed). • make all reasonable attempts to let impacted individuals know and help them recover their ID and remediate impacted services.
System Administrator **will**	• assess the notification and undertake an investigation where needed to identify all Participating Relying Party services that may have consumed the digital IDs • will notify each of the Participating Relying Parties.
ISP **must**	• follow their fraud management process • make all reasonable attempts to let impacted individuals know and help them to recover their ID and remediate impacted services • notify the System Administrator of the outcome.

Scenario 3	**Identity Service Provider detects suspected fraudulent identities**
Details	An ISP detects suspected fraud with digital IDs provisioned by their service. The security measures in place stops them knowing if the digital IDs have interacted with any Participating Relying Party services.
ISP must **immediately**	• follow their fraud management process • prevent the ongoing use of suspicious digital IDs • notify the System Administrator (and submit a Request for Information if needed) • work collaboratively with the System Administrator to make all reasonable attempts to let impacted individuals know and help them to recover their ID and remediate impacted services.
System Administrator **will**	• supply Participating Relying Parties with a pairwise identifier (RP Link) to locate specific user records • if required, facilitate conferences between entities.
Participating Relying Parties **must**	• follow their fraud management process • work collaboratively with the System Administrator and make all reasonable attempts to let impacted individuals know and help them to recover their ID and remediate impacted services • notify the System Administrator of the outcome.
Scenario 4	User identifies unauthorised access or use of digital ID
Details	A user discovers their digital ID has been accessed by an unknown device. The individual reports this to their Identity Service Provider (ISP).
ISP must **immediately**	• follow their fraud management process • prevent the ongoing use of the user’s digital ID • notify the System Administrator (and submit a Request for Information if needed) • help individuals impacted by fraud to recover their ID (including reproofing the digital ID and resetting the authentication credentials).
System Administrator **will**	• supply Participating Relying Parties with a pairwise identifier (RP Link) to locate specific user records • if required, facilitate conferences between entities.
Participating Relying Parties **must**	• follow their fraud management process • work collaboratively with the System Administrator and make all reasonable attempts to let impacted individuals know and support them to recover their ID and remediate impacted services • notify the System Administrator of the outcome.
Scenario 5	Employee accessing digital ID records without authorisation
Details	An entity identifies an employee has accessed records in the organisation’s digital ID service without authorisation.
Participating Relying Parties must **immediately**	• follow their fraud management process • notify the System Administrator (and submit a Request for Information if needed) • consider whether a notifiable data breach has, or is likely to have, occurred and if so, also report this to both the Digital ID Regulator and the OAIC.
System Administrator **will**	• undertake the relevant investigation to identify impacted systems and notify impacted entities • if required, facilitate conferences between entities.

Maintenance of the system wide Fraud Risk Management Plan

The Fraud Risk Management Plan (FRMP) identifies the shared risks to the AGDIS. The FRMP is a living document and is maintained by the System Administrator in collaboration with entities. All entities must conduct regular fraud risk assessments for their participating service (including for any substantial changes in structure, functions or activities).

Where fraud is identified, an entity must consider whether it is a shared risk. Potential shared risks need to be reported to the System Administrator using the Fraud and Cyber Security Risk Reporting form (please email AGDIS.Administrator@servicesaustralia.gov.au for a copy of this form). Once mandatory fields are completed, return the completed form to AGDIS.Administrator@servicesaustralia.gov.au.

The System Administrator will assess and, if required, table the risk at the Cyber Security, Fraud Control Advisory Group. The group will assess the risk and determine if it is included in the FRMP and/or Security Risk Management Plan.

5.5 Cyber security management and incident response

Participating entities cyber security requirements

Accredited Entities must follow the protective security controls detailed in Part 4.1 of the Accreditation Rules. This includes having a comprehensive system security plan as detailed in Rule 4.12.

Participating Relying Parties must follow the requirements in Chapter 3 of the Rules. This includes having a written cyber security plan as per Rule 3.3(2)(a).

Participating entities general obligations

Rule 4.2 of the Rules sets out the requirements for **Accredited Entities** and **Participating Relying Parties** to report a cyber security incident. Failure to adhere to these requirements may incur a civil penalty of 1,500 penalty units as per section 78 of the Act.

What is a cyber security incident?

> A cyber security incident is an act, event or circumstance that has a significant probability of compromising the AGDIS and involves either:
>
> - unauthorised access, modification or interference to a system, service or network connected to the AGDIS, or
> - unauthorised impairment to availability, reliability, security or operation of a system, service or network connected to the AGDIS.

Role of the System Administrator

The System Administrator:

- helps transfer information between entities to investigate security, privacy and fraud incidents
- coordinates entity responses to incidents, ID theft, disaster recovery and other relevant issues
- undertakes inquiries and investigations in the AGDIS (which includes cyber security)
- reports back to the entities on results of investigations and on cyber security threats to the AGDIS identified by wider intelligence gathering activities (including external intelligence and commercial partners).

Detecting cyber security incidents

The availability of appropriate data sources is a core element of detecting and investigating cyber security incidents. Below are some of the data sources participating entities can use.

Data source	Useful for
Domain name system logs	Identifying attempts to resolve malicious domains or Internet Protocol (IP) addresses. Can indicate an exploitation attempt or successful compromise.
Email server logs	Identifying users targeted with spear-phishing emails and identifying the initial vector of a compromise.
Operating system event logs	Tracking process execution, file/registry/network activity, authentication events, operating system-created security alerts and other activity.
Security software and appliance logs	Identifying anomalous or malicious activity. Can indicate an exploitation attempt or successful compromise.
Virtual Private Network and remote access logs	Identifying unusual source addresses, times of access and logon/logoff times associated with malicious activity.
Web proxy log	Identifying Hypertext Transfer Protocol-based vectors and malware communication traffic.

Reporting suspected cyber security incidents to the System Administrator

Participating entities must report suspected or confirmed digital ID fraud to the System Administrator. The System Administrator will undertake an investigation where required and notify all potentially impacted entities of the fraud.

As per Rule:

- 4.2 (4) of the Rules, participating entities must notify the System Administrator as soon as practicable after, and no later than one business day after, they become aware that an incident has occurred or reasonably suspects that an incident has occurred.
- 4.2 (5) of the Rules, this notification may be given orally, however if it is given orally, written notification must be given no later than 3 business days after the oral notification. Written notification is required via the Administrator Portal.

Where there are reasonable grounds to believe that there has been an eligible data breach (within the meaning of the Privacy Act), **Accredited Entities** that are APP entities, must give the Information Commissioner a statement that complies with section 26WK of the Privacy Act and give a copy of that statement to the Digital ID Regulator.

Where a cyber security incident is impacting on the availability of the AGDIS, the incident **must** be reported as outlined for an IT system incident in **Section 5.1** of this Handbook.

> The System Administrator does not provide cross-system proactive detection. As a result, the System Administrator relies on participating entities promptly reporting cyber security incidents to ensure effective cross-system cyber security management.

Reporting investigation outcomes to the System Administrator

Where the System Administrator notifies a participating entity of a confirmed cyber security incident, that participating entity must investigate. Once investigations are complete (or when the facts are known), they need to notify the System Administrator of the outcome.

Scenarios for reporting cyber security incidents

The following scenarios show the types of cyber security incidents that need to be reported:

Scenario 1	**Phishing campaign using entity's branding targeting AGDIS users**
Details	A phishing campaign using an entity's branding, targeting AGDIS users and aiming to compromise personal information.
Entity must **immediately**	• follow the incident reporting plan as per their internal incident management process • identify if any of the affected accounts were linked to a digital ID • if affected account were linked to a digital ID, prevent the ongoing use of any compromised digital IDs • if affected accounts were linked to a digital ID, notify the System Administrator, (and submit a Request for Information if needed) • investigate the incident.
Scenario 2	Compromise or corruption of information
Details	A compromise or corruption of entity service data or information.
Entity must **immediately**	• follow the incident reporting plan as per their internal incident management process • prevent ongoing use of the account where an individual may be at risk • notify the System Administrator, (and submit a Request for Information if needed) • investigate the incident.
The ISP must **immediately**	• prevent the ongoing use of any compromised digital IDs • investigate the incident.
The System Administrator **will**	• undertake an investigation if needed to identify the ISP who provisioned the digital ID • notify the ISP.
Affected entities **must**	• work together and make all reasonable attempts to let impacted individuals know • notify the System Administrator of the outcome.
Scenario 3	Unauthorised access or intrusion
Details	There is an unauthorised access or intrusion to the AGDIS.
Entity must **immediately**	• follow the incident reporting plan as per their internal incident management process • prevent the ongoing use of any compromised digital IDs • notify the System Administrator, (and submit a Request for Information if needed) • investigate the incident • notify the System Administrator of the outcome.
Scenario 4	Malicious software in entity system
Details	An intentional or accidental introduction of malicious software into an Accredited Entity or Participating Relying Party system.
Entity must **immediately**	• follow the incident reporting plan as per their internal incident management process • prevent the ongoing use of any compromised digital IDs • notify the System Administrator, (and submit a Request for Information if needed) • investigate the incident and notify the System Administrator of the outcome.

Scenario 5	Successful denial of service attack
Details	An attempted or successful denial of service attack against an Accredited Entity or Participating Relying Party system.
Entity must **immediately**	• follow the incident reporting plan as per their internal incident management process • prevent the ongoing use of any compromised digital IDs • notify the System Administrator, (and submit a Request for Information if needed) • investigate the incident • notify the System Administrator of the outcome.
Scenario 6	**Suspicious network activity**
Details	A suspicious or unauthorised network activity against an Accredited Entity or Participating Relying Party system.
Entity must **immediately**	• follow the incident reporting plan as per their internal incident management process • prevent the ongoing use of any compromised digital IDs • notify the System Administrator, (and submit a Request for Information if needed) • investigate the incident and notify the System Administrator of the outcome.
Scenario 7	Successful exploitation of a vulnerability
Details	A successful exploitation of a vulnerability in the Accredited Entity or Participating Relying Party system.
Entity must **immediately**	• follow the incident reporting plan as per their internal incident management process • prevent the ongoing use of any compromised digital IDs • notify the System Administrator, (and submit a Request for Information if needed) • investigate the incident • notify the System Administrator of the outcome.
Scenario 8	**Credential stuffing campaign targeting System users**
Details	A credential stuffing campaign where user credentials obtained from other data breaches are used to obtain unauthorised access to System user accounts.
Entity must **immediately**	• follow the incident reporting plan as per their internal incident management process • identify if any of the affected accounts were linked to a digital ID • if affected accounts were linked to a digital ID, prevent the ongoing use of any compromised digital IDs • if affected accounts were linked to a digital ID, notify the System Administrator, (and submit a Request for Information if needed) • investigate the incident.

Participating entities are also encouraged to report cyber security incidents to the Australian Cyber Security Centre (ACSC).

It should be noted there may be civil penalties applicable for entities that fail to comply with reporting these incidents.

Maintenance of the system wide Security Risk Management Plan

The Security Risk Management Plan (SRMP) identifies the shared risks to the AGDIS. Shared risks affect more than one participating entity in the AGDIS.

The SRMP is a living document and is maintained by the System Administrator in collaboration with entities. All entities need to conduct regular security risk assessments for their digital ID service (including for all substantial changes in structure, functions or activities).

Where cyber security risks are identified, an entity must consider whether it is a shared risk. Potential shared risks need to be reported to the System Administrator using the Fraud and Cyber Security Risk Reporting form (please email AGDIS.Administrator@servicesaustralia.gov.au for a copy of this form). Once mandatory fields are completed, return the completed form to AGDIS.Administrator@servicesaustralia.gov.au.

The System Administrator will assess and, if required, table the risk at the Cyber Security, Fraud Control Advisory Group. The group will assess the risk and determine if it is included in the FRMP and/or SRMP.

Accredited Entities Essential Eight requirements

Accredited Entities should regularly monitor their Essential Eight maturity. This maturity comes from treatments to address risks. Implementing treatments helps mitigate risks to the confidentiality and integrity of digital ID information.

Accredited Entities may be required to report their Essential Eight maturity to the Digital ID Regulator as part of their accreditation or annual review process.

For more information, visit cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight

Australian Signals Directorate’s (ASD) Australian Cyber Security Partnership Program

The ASD Partnership Program enables Australian organisations and individuals to engage with the ASD and fellow partners, drawing on collective understanding, experience, skills and capability to lift cyber resilience across the Australian economy, and is delivered through the ASD’s ACSC and fellow partners.

ASD’s Network Partnership is available to organisations with responsibility for the security of a network or networks (either your own or on behalf of customers), and academic, research and not-for-profit institutions with an active interest and expertise in cyber security.

The program offers:

- threat intelligence and enhanced situational awareness
- collaboration opportunities
- resilience-building activities
- the ACSC network.

To lift cyber resilience across the AGDIS, participating entities are encouraged to become an ASD partner. For more information, visit cyber.gov.au/partnershipprogram

The System Administrator may also use external intelligence partners for threats that may impact the wider system.

5.6 Supporting individuals affected by digital ID fraud or cyber security incidents

All entities must make reasonable efforts to notify and provide support to individuals affected by a digital ID fraud or a cyber security incident. Entities can choose to provide this support directly or via a third party.

> **Note:** contact information for affected individuals is **only** provided by the entity to the System Administrator if the entity has **both**:
>
> - confirmed the individual's ID, **and**
> - obtained trusted contact details for the individual.
>
> This is important because contact information on a compromised digital ID record **cannot** be considered trusted.

When notifying the System Administrator of a digital ID fraud or cyber incident, Rule 4.2 of the Rules sets out the requirement to include information on whether an individual affected by an incident has been informed (and if so when) or not informed (and if so why).

Tips for getting information from affected individuals

During initial contact with an individual, it is important to check:

- **Have they previously set up a digital ID account?**
  You can use prompts such as describing the process to set it up, documents they may have needed to type in or scan, or a specific reason they may have needed to set up the digital ID. You can also ask them to check their phone for digital ID apps, such as myID and their email accounts for notification emails.
- **If they did set the account up, when was the last time they used it to log into a participating service, and what services did they access?**
  This information could be in emails, on apps, or tied to the reason they set up the digital ID.

Collect information about their specific digital ID use and more general online habits.

These questions will allow investigators across participating entities to narrow down when and how the account may have been compromised.

> **Note:** it is important to explain the difference between a digital ID and a user's login details for a service. For example, logging into myGov using a username and password versus logging into myGov using a digital ID.

Multiple entities providing assistance

When contacting the individual, entities need to be aware that multiple organisations could be contacting and assisting the same individual simultaneously. Entities are encouraged to approach the messaging as one part of a coordinated response. This ensures a professional approach and helps maintain public confidence in the AGDIS. One way to do this is to acknowledge the work of other entities: "I understand you spoke with (name of notifying entity) on Monday".

This information will be shared by the System Administrator with relevant entities where available.

Entities should provide information on the next steps and a basic overview of the process, including publicly available resources on the digitalidsystem.gov.au website. This ensures the affected individuals understand:

- multiple organisations are working together to assist them
- the AGDIS is working hard in the background, even if it isn't obvious from the outside
- their assistance is valuable, and their information is important to our investigations.

Where relevant, entities should provide the individual with a referral to external support (such as IDCARE) and consider assisting the individual to obtain a Commonwealth Victims' Certificate.

Role of the Entity and the System Administrator

Once an entity notifies the System Administrator of an incident, the System Administrator will undertake an investigation to identify other affected entities. The System Administrator will then communicate information to any affected entities (including information about the affected individual if known).

Where possible, entities will contact affected individuals and provide:

- service-specific remediation
- broader support for ID crime

Entities report back to the System Administrator and include any information about the incident and contact with the affected individual.

The System Administrator provides collected trusted contact details for affected individuals to entities (where these were not known).

5.7 AGDIS System Administrator Data Sharing Principles

The System Administrator's authority to request information, and record keeping requirements for participating entities and former participating entities, are detailed in sections 134-136 of the Act.

The AGDIS System Administrator Data Sharing Principles describes:

- the relevant data attributes or elements collected and retained by the System Administrator for the purposes of performing its powers and functions under the Act
- the purpose for which the System Administrator stores and discloses data collected and retained, or requests data with/from:
    - Participating Entities,
    - The Digital ID Regulator as represented by the Australian Competition and Consumer Commission (ACCC),
    - The Information Commissioner as represented by the Office of the Australian Information Commissioner (OAIC),
    - The Data Standards Chair (DSC) and the Data Standards Body (DSB)
    - Courts or Tribunals
    - Law Enforcement Agencies, and
    - The Minister for Finance (the Minister).

For a copy of the AGDIS System Administrator Data Sharing Principles, please refer to the digitalidsystem.gov.au website.