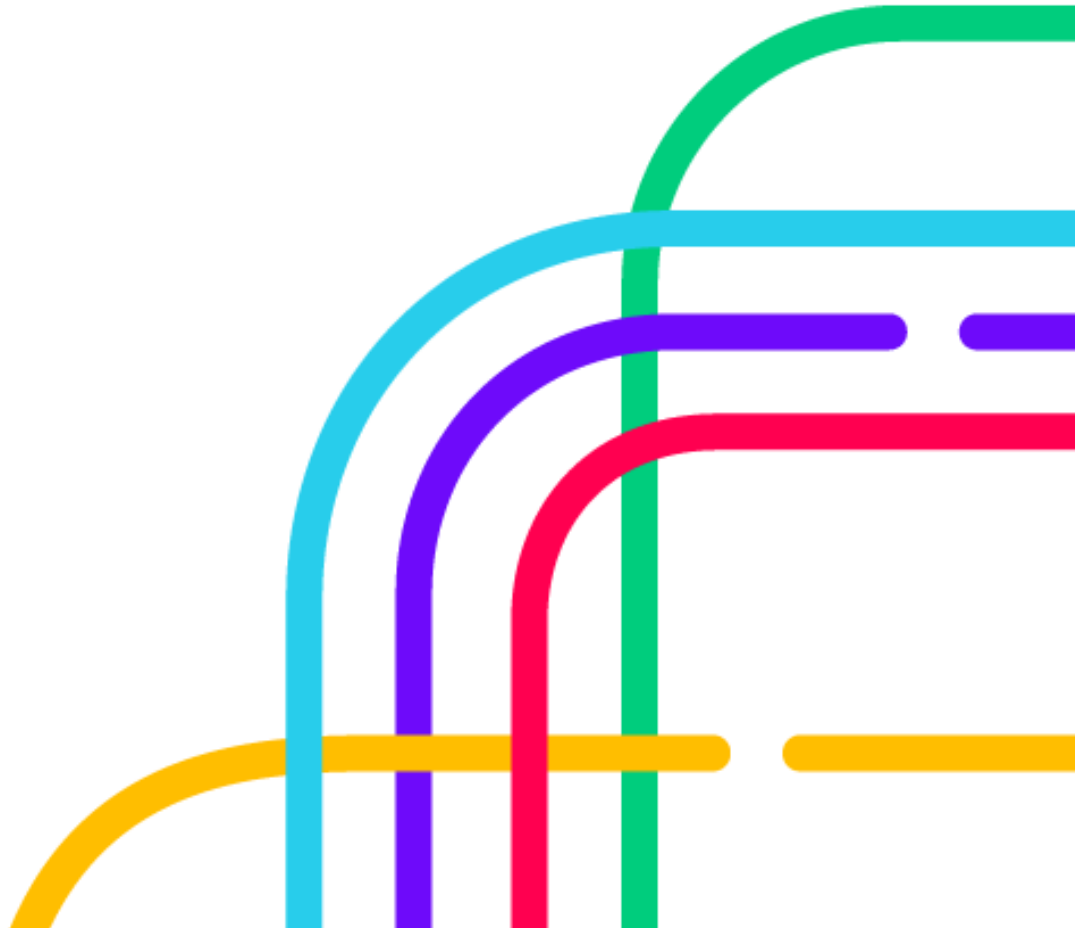
dspanz. digital service providers australia new zealand

Security Incident Reporting

Comprehensive Guide for Australian Digital Service Providers (DSPs)

Version 1.0

Published 25 November 2025



Contents

Introduction

The Security Incident Reporting: Comprehensive Guide for Australian Digital Service Providers (DSPs) aims to help software providers navigate their obligations to report security incidents.

DSPs often capture, transmit and store sensitive personal and financial information as part of the software products and services they provide to their customers. Many DSPs also operate in regulated environments or interact with digital services provided by government agencies.

DSPs often capture, transmit and store sensitive personal and financial information as part of the software products and services they provide to their customers. Many DSPs also operate in regulated environments or interact with digital services provided by government agencies.

As a result, DSPs may have legislative, regulatory or “conditions of access” obligations to report security incidents. These reporting obligations vary in their definitions, thresholds, information requirements and reporting timeframes. It can be complex for DSPs to navigate multiple reporting obligations in the event of an incident.

This guidance explores security incidents, what makes them reportable and outlines the common security incident reporting obligations that may apply to DSPs operating in Australia, including:

- Notifiable Data Breaches (NDB) Scheme
- ATO’s DSP Operational Security Framework
- APRA Prudential Standard CPS 234: Information Security
- ASX-Listed Entities Continuous Disclosure Requirements
- Critical Infrastructure Cyber Security Incident Reporting
- Mandatory Ransomware and Cyber Extortion Payment Reporting.

While this guide provides an overview of common reporting obligations and expectations, it is important for DSPs to consider their unique circumstances and stay up to date with changes and or new obligations that may arise.

DSPANZ will continue to update this guidance as regulatory settings develop or new reporting obligations are introduced.

Definitions

Digital Service Provider: Digital Service Providers, or DSPs, create, sell, and use software solutions to securely capture, transmit, and share information. These solutions are commonly used in the day to day management of a business and its employees.

Personal Information: Personal information includes a broad range of information, or an opinion that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances[1]. Personal information is also known as Personally Identifiable Information (PII).

Personal information may include:

- An individual's name, signature, address, phone number or date of birth
- Credit information
- Employee record information
- Internet Protocol (IP) addresses
- Location information from a mobile device
- Photographs
- Sensitive information
- Voice print and facial recognition biometrics.

Reportable Incident: A reportable incident is a security event that meets specific criteria, requiring formal notification.

Security Incident: A security incident is any event that compromises the confidentiality, integrity, or availability of data, systems, or services.

Tax File Numbers [2] [3]**:** A Tax File Number (TFN) is a personal reference number in the tax and superannuation system generated by the Australian Taxation Office (ATO) that is:

- A unique number (usually 9 digits)
- An important part of an individual's identity
- Issued to an individual for life.

[1] OAIC - What is personal information?
[2] ATO - What is a tax file number?
[3] OAIC - Your tax file number

Critical Infrastructure: Assets or services considered essential for the functioning of the economy, health, safety or security of Australians as defined under the *Security of Critical Infrastructure Act 2018 (SOCI)*.

What is a Security Incident?

A security incident is any event that compromises the confidentiality, integrity, or availability of data, systems, or services.

Examples of security incidents can include:

- **Data breaches:** Unauthorised access, disclosure or loss of sensitive information.
- **Unauthorised access:** An individual or entity gains access to data or systems without permission.
- **Credential misuse:** Employees or contractors with legitimate access to data or systems misuse this privilege to view, change or take copies of data.
- **Ransomware or malware:** Ransomware or malicious software designed to block access to data or systems without permission.
- **Distributed Denial of Service (DDoS) attacks:** Flooding a network with excessive traffic, causing disruptions and limiting system availability.

Reportable incidents

A reportable incident is a security event that meets specific criteria set out by legislative or regulatory requirements or security frameworks that require formal notification.

While the criteria for a reportable incident may differ across requirements, an incident is generally considered reportable if:

- The incident involves sensitive data such as PII, TFNs or financial records;
- Critical systems or services experience outages or loss of functionality; or
- The incident meets defined thresholds.

Reporting Obligations

There are several security incident reporting obligations that may apply to DSPs operating in Australia.

This section outlines the common security incident reporting obligations for DSPs, provides guidance on managing multiple reporting obligations during an incident and highlights some examples.

Find a list of relevant legislation and requirements, further resources and a table summarising the requirements of common reporting obligations in the Appendix.

Common Security Incident Reporting Obligations for DSPs

The following information outlines the common security incident reporting obligations for DSPs and highlights:

- What makes an incident reportable
- How incidents can be reported
- When should incidents be reported
- Where to find more information.

Notifiable Data Breaches (NDB) Scheme:

DSPs covered by the *Privacy Act 1988* must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach involving personal information is likely to result in serious harm under the NDB scheme.

Generally, DSPs with an annual turnover of more than $3 million or those handling Tax File Numbers (TFNs) are covered by the Privacy Act and must therefore comply with the NDB scheme. The OAIC provides further guidance on how the Privacy Act applies.

As the OAIC also oversees the Consumer Data Right (CDR) and Digital ID systems. Accredited Data Recipients (ADRs) in the CDR system and accredited entities in the Digital ID system are required to follow the NBD scheme.

Organisations generally have 30 calendar days from becoming aware of a data breach to assess whether it is likely to result in serious harm. If the data breach is expected to result in serious harm, organisations should then prepare a statement to report via the Notifiable Data Breach Form and notify individuals as soon as practicable. A copy of the Notifiable Data Breach Form has been published for "training purposes", allowing organisations to understand the information required.

The statement shared with the OAIC and notifications to individuals must include:

- Your organisation's name and contact details
- A description of the data breach
- The kinds of information involved
- Recommendations about the steps individuals should take in response to the data breach.

More detailed information about the NDB scheme, including identifying eligible data breaches, assessing a suspected data breach, notifying individuals, what to include in a statement, and examples, is available on the OAIC's website.

For more general information about the NDB scheme and data breaches under the Privacy Act, visit the following:

- When to report a data breach
- Reporting a data breach
- Data breach preparation and response.

ATO DSP Operational Security Framework (OSF):

DSPs with software that reads, stores, modifies, or routes any taxation, accounting, payroll, business registry, or superannuation data that connects:

- Directly to ATO digital services
- Indirectly to the ATO via a Sending Service Provider (SSP) for payroll services
- Indirectly to the ATO via a gateway for superannuation services or SuperStream

Must comply with the OSF and report data breaches involving PII.

Data breaches should be reported immediately from the time a DSP becomes aware that PII data has been breached, or ideally within a few hours, to allow the ATO to implement preventative actions.

DSPs must report data breaches via the incident report form in the DSP service desk within Online Services for DSPs. The following information (when known) must be reported:

- Appropriate contact person (specialist IT security/fraud representative)
- Nature of the breach
- Number of affected records
- Date and timestamp
- Session ID reference
- Host Services (Internet Service Provider)/IP address
- Device ID (ESID) if available
- Identifiable information (name/address/biographical information)
- Whether TFN details were exposed
- Product name and type (desktop or cloud)
- What format the data is in (for example, CSV or encrypted).

More information about data breaches, what to report and how to report is available on the ATO's software developer website.

Australian Prudential Regulation Authority (APRA) Prudential Standard CPS 234: Information Security:

DSPs regulated by APRA must notify them about material information security incidents and material information security control weaknesses, as outlined in Prudential Standard CPS 234: Information Security and the accompanying Prudential Practice Guide.

Regulated entities must notify APRA as soon as possible and no later than 72 hours after becoming aware of an information security incident that:

- Materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; or
- Has been notified to other regulators, either in Australia or other jurisdictions.

Entities must also notify APRA as soon as possible, but no later than 10 business days, after becoming aware of a material information security control weakness that the entity expects to be unable to remediate in a timely manner.

ASX-Listed Entities Continuous Disclosure Requirements:

DSPs listed on the Australian Securities Exchange (ASX) must immediately notify the ASX if they become aware of information that a reasonable person would expect to

have a material impact on the price or value of their securities. This can include cybersecurity incidents, depending on the nature and impact of the incident.

Chapter 3 of the ASX Listing Rules provides more information about the continuous disclosure requirements. The complete ASX Listing Rules, along with supplementary information, are available on the ASX website.

Critical Infrastructure Cyber Security Incident Reporting:

DSPs that are regulated under Part 2b of the *Security of Critical Infrastructure Act 2018 (SOCI)* may be subject to mandatory cyber incident reporting requirements.

If entities become aware that a critical cybersecurity incident has occurred or is occurring and the incident has, or is having, a significant impact on the availability of their asset, they must notify the ASD's ACSC within 12 hours of becoming aware of the incident.

Other cyber security incidents that have occurred, or are occurring, and the incident has had, is having, or is likely to have a relevant impact on an entity's asset, they must notify the ASD's ACSC within 72 hours after becoming aware of the incident.

Entities are required to report the following:

- Contact details of the person making the report
- Organisation details
- Date and time the incident was identified
- Whether the incident is ongoing
- Which systems and data are being impacted
- Whether the incident was identified by the organisation or a third party
- Type of incident.

More information about reporting critical infrastructure cybersecurity incidents, along with the reporting form, is available on the ASD's ACSC website.

Mandatory Ransomware and Cyber Extortion Payment Reporting:

Under the *Cyber Security Act 2024,* DSPs with an annual turnover of $3 million or more within the last financial year must report to the Federal Government if they make a ransomware or cyber extortion payment within 72 hours

This reporting requirement applies only when an entity makes a ransomware or cyber extortion payment, or is aware that a payment has been made on its behalf. Reports are required if payments have not been made.

Entities are required to report ransomware and cyber extortion payments to the ASD's ACSC via the form on their website. Information that must be reported includes the

following when it is known:

- Organisation details
- Details about the incident, including its impact on the reporting entity
- Details about the demand made by the extorting entity
- Details about the payment
- Communications with the extorting entity
- Additional information that may assist in the response, mitigation or resolution.

The Department of Home Affairs provides more information about the mandatory ransomware and cyber extortion obligation in the following two resources:

- Factsheet
- How to make a report.

While it is not a mandatory requirement, the Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC) enables the reporting of cybercrime, incidents, or vulnerabilities for individuals, organisations, and government departments or agencies, and provides support during cybersecurity incidents.

Reporting is encouraged as soon as an incident is detected to help the ASD provide the appropriate technical support and advice.

DSPs can report incidents via the form available on the ACSC website.

Managing Multiple Reporting Obligations During an Incident

Some security incidents may require DSPs to notify more than one regulator or government agency, which can create challenges, as each obligation has different thresholds, reporting timeframes and information requirements.

DSPs that interact with or are regulated by multiple government agencies must navigate different reporting thresholds, timeframes and information requirements under each security incident reporting obligation. When an incident needs to be reported under multiple obligations, it can be complex for DSPs to understand what needs to be reported, when it needs to be reported, and to whom it should be reported.

When an incident occurs, DSPs may need to submit reports to multiple agencies simultaneously. While the details required in a report and its timing may differ between obligations, common information required typically includes a combination of the following:

- A summary of the incident
- Type/s of data affected
- Timeline of events
- Systems impacted
- Number of individuals affected
- Remediation actions
- Supporting documentation.

DSP should be familiar with the obligations that apply to their organisation, products and services, and be prepared to manage situations where multiple reporting requirements overlap.

Being prepared and coordinating a response across different reporting obligations will help DSPs meet requirements efficiently and consistently. To support this, DSPs should:

- Understand the reporting obligations that apply to their organisation, including legislative, regulatory, sector-specific or government agency requirements.
- Map out obligations in advance and consider how they could interact if an incident were to occur.
- Establish clear escalation and communication channels within your organisation to ensure reports are made within the required timeframes and support sharing follow-up information.
- Keep accurate records of incidents, reports and decisions made for your own record-keeping purposes and to inform future incident responses and reports
- Seek advice if you are unsure about whether an incident is reportable, particularly where obligations may overlap.
- Develop and maintain an incident response plan that captures these key points and test it regularly.

Example 1: Misconfigured Cloud Storage (PII Data Breach)

A payroll and HR software provider discovered that a misconfigured cloud-storage bucket allowed public access to employee onboarding documents. Files included scanned passports, driver's licences, Medicare cards and TFN declarations. At least one external IP address accessed the documents.

Assessment:

- Data exposed included identity documents and TFNs.
- Files were unencrypted and accessed externally, meeting the definition of an eligible data breach.
- The presence of TFNs and identity records means obligations apply across multiple regulators.

Reporting Obligation	What To Report	Reporting Timeframes
OAIC (NDB Scheme)	Notify OAIC and affected individuals	Within 30 days.
ATO (OSF)	Immediate notification due to TFN compromise.	Within hours.
ASX	If listed, assess continuous disclosure obligations.	Immediately, if material.

Actions for DSPs:

- Contain exposure by locking storage, auditing logs, confirm what data was accessed and duration of access.
- Collect required details for reports (incident summary, data types, individuals affected) and maintain consistent incident information.
- Notification content must include a description of the breach, types of data involved, recommendations for individuals, and a contact point.
- Fix misconfiguration, test all storage for exposure, and implement monitoring.

Example 2: Superannuation Clearing House Ransomware Attack

A DSP operating a superannuation clearing house was impacted by a ransomware attack. Contribution files were encrypted and data was exfiltrated, including TFNs, bank account details and contribution information. Payment processing to funds was delayed.

Assessment:

- Exfiltrated data included TFNs and financial information.
- Encryption caused service disruption and delays.
- The incident meets reporting thresholds across multiple obligations

Reporting Obligation	What To Report	Reporting Timeframes

OAIC (NDB Scheme)	Notify OAIC and affected individuals	Within 30 days.
ACSC (SOCI Act)	Notify ACSC, if designated as critical infrastructure	Within 12–72 hours.
ATO (OSF)	Immediate notification due to TFN and contribution data compromise	Within hours.
ASX	If listed, assess continuous disclosure obligations.	Immediately, if material.

Actions for DSPs:

- Contain the attack, confirm what data was accessed and restore affected systems.
- Collect required incident details and ensure reporting is consistent across agencies.
- Notify employers about delays and provide updates on remediation.
- Review controls, rotate credentials and validate the integrity of restored contribution files.

Example 3: Accidental Disclosure of Tax File Number

A DSP accidentally emailed a payroll spreadsheet containing TFNs to the wrong employer contact. The error was identified shortly after the email was sent, and retrieval was attempted immediately.

Assessment:

- TFNs and payroll information were unintentionally disclosed.
- Harm depends on whether the file was accessed, saved or shared.
- ATO OSF reporting is required and NDB Scheme obligations may apply.

Reporting Obligation	What To Report	Reporting Timeframes
OAIC (NDB Scheme)	If serious harm is likely.	Within 30 days.
ATO (OSF)	TFN disclosure.	Within hours.
ACSC	DSP may choose to report for situational awareness.	**Voluntary**, as soon as detected
ASX	If listed, assess continuous disclosure obligations.	Immediately, if material.

Actions for DSPs:

- Contact the unintended recipient, request deletion and obtain written confirmation.
- Conduct a serious harm assessment and document findings.
- Report to the ATO OSF and review internal handling processes.
- Notify affected individuals if required under the NDB Scheme.

Conclusion

Security incidents can escalate quickly, and determining the correct reporting requirements is critical to an effective response. By understanding the thresholds and triggers across multiple reporting agencies, DSPs can act with confidence and ensure their response meets all necessary requirements.

This guide provides a consolidated reference to assist DSPs in assessing incidents, identifying relevant obligations, and reporting within mandated timeframes. While each incident will have unique characteristics, the frameworks and examples in this document offer a clear starting point for determining the appropriate course of action. DSPs are encouraged to utilise this guidance in their internal response processes.

DSPANZ will continue to update this resource as regulatory settings evolve and as new guidance becomes available. Ensuring timely, accurate and transparent reporting strengthens the resilience of the entire digital services sector and reinforces trust across industry and government.

DSPANZ encourages DSPs to stay informed about the incident reporting obligations that apply to them and how these may change in line with the evolving threat landscape.

Appendix 1 - Relevant Legislation and Requirements

Legislation, Regulations and Requirements
ATO DSP Operational Security Framework
Australian Privacy Principles
Chapter 3 of the ASX Listing Rules
Cyber Security Act 2024
Mandatory Ransomware and Cyber Extortion Reporting Factsheet
Privacy Act 1988
Privacy Amendment (Notifiable Data Breaches) Act 2017
Prudential Standard CPS 234: Information Security
Security Standard for Add-on Marketplaces
SOCI Act 2018, Part 2A
Tax File Number Rule

Appendix 2 - Further Information and Resources

Organisation or Agency	Resource
ACSC	Resources Library
ACSC	Ransomware
APRA	Prudential Practice Guide
APRA	Prudential Practice Guide 235 Managing Data Risk
ASD	Ransomware Extortion Reporting Guide
ATO	DSP Operational Security Framework
ATO	What is a Tax File Number
DSPANZ	Security Standard for Add-on Marketplaces
OAIC	Notifiable Data Breach Form - For Training Purposes
OAIC	Cyber Security Incident Response Planning: Practitioner Guidance
OAIC	Notifiable Data Breaches

OAIC	Guide to securing personal information
OAIC	Data Breach Preparation and Response
OAIC	Preventing, Preparing For and Responding to Data Breaches
OAIC	Your Tax File Number
OAIC	What is Personal Information
OAIC	About the Notifiable Data Breaches Scheme
OAIC	The Tax File Number Rule
OAIC	Rights and Responsibilities Under the Privacy Act
OAIC	When to Report a Data Breach
OAIC	Report a Data Breach

Appendix 3 - Acronyms

ACCC	Australian Competition and Consumer Commission
ACSC	Australian Cyber Security Centre
APRA	Australian Prudential Regulation Authority
ASD	Australian Signals Directorate
ASX	Australian Securities Exchange
ATO	Australian Taxation Office
CDR	Consumer Data Right
DSPANZ	Digital Service Providers Australia New Zealand
DSP	Digital Service Provider
TFN	Tax File Number
OSF	Operational Security Framework
OAIC	Office of the Australian Information Commissioner
SSP	Sending Service Provider
SOCI	Security of Critical Infrastructure
PII	Personally Identifiable Information
NDB	Notifiable Data Breach

Appendix 4: DSP Notification Requirements

Regulator or Framework	Obligation	Notification Trigger	Notification Timeframe	Trigger Type	Urgency Deadline (Hrs)
ASX	ASX Ch. 3 Listing Rule 3.1	Material market-sensitive impact	Immediately once aware	Automatic (market-sensitive disclosure)	Immediate / 0
OAIC/ACCC	OAIC CDR Breach Reporting CDR – Sponsored Affiliate	Breach of CDR data by a sponsored affiliate	Immediately to sponsor (who then notifies OAIC)	Automatic (CDR-affiliate breach)	Immediate / 0
Australian Taxation Office (ATO)	Operational Security Framework	Any unauthorised access or security incident affecting ATO data	As soon as practicable (ideally within a few hours)	Automatic (unauthorised access)	Immediate / 0
SOCI	SOCI Act 2018, Part 2A	Significant cyber incident impacting critical infrastructure	12 hours for significant incidents; 72 hours for other incidents	Automatic (CI incident)	Short / (12h -72h)
APRA	APRA CPS 234	Material information security incident or control weakness	As soon as practicable, no later than 72 hours	Automatic (material incident/ weakness)	Time-bound / 72h
Cyber Security Act 2024	Ransomware Extortion Payment Reporting	Any ransomware or cyber-extortion payment	As soon as practicable, no later than 72 hours	Automatic (ransomware/extortion payment)	Time-bound / 72h

Any breach of personal information likely to cause serious harm	Notifiable Data Breach	Any breach of personal information likely to cause serious harm	As soon as practicable, no later than 30 days	Internal assessment (serious harm test)	Assessment-Based
CDR/NDB	Notifiable Data Breach	Any breach of protected data causing likely serious harm	As soon as practicable, no later than 30 days, part of NDB.	Internal assessment (harm test)	Assessment-Based