Government of Western Australia
Department of Transport
and Major Infrastructure

Empowering a thriving community

Information Breach Procedures

Prepared for the Department of Transport and Major Infrastructure

Prepared by Information Governance | Business Information Systems

Information Breach Procedures

Document Control

Objective File Number	DT/26/03145
Objective Document ID.	A24848392
Version Number	0.1
Date	26/11/2026

Revision History

Next Review Date:

Version No.	Date	Summary of Changes	Author / Editor
			Suzana Gligorov

Approvals

Name	Position title	Date	Approval Reference
Anu Sutharshan	Director Information Governance		

Table of Contents

INFORMATION BREACH PROCEDURES 1

1. Purpose 4
2. Scope 4
3. Definitions and terms 4
4. Roles and Responsibilities 11
5. Notifiable information breaches 13
5.1 Examples 13
6. Responding to and reporting on an information breach 13
6.1 Initial detection and triage 14
6.2 Contain 14
6.3 Assess and mitigate 15
6.4 Notify 16
6.5 Review 17
7. Shared information breaches – Overview 19
7.1 Managing shared information breaches – Additional information 19
8. Recordkeeping 20
8.1 Document creation 20
8.2 Register of Information Breaches 20
8.3 Annual Report 20
9. Review and continuous improvement 20
10. Communication Strategy 21
11. Related Information 21
Appendix 1. Information Breach Notification Form 22
Appendix 2. Information Breach Assessment and Resolution Form 24
Appendix 3. Quick Reference Checklists: Shared Information Breaches 27

Information Breach Procedures

1. Purpose

This document sets out the procedures adopted by the Department of Transport and Major Infrastructure (DTMI) for managing suspected or assessed notifiable information breaches, ensuring compliance with Part 2 Division 6 of the *Privacy and Responsible Information Sharing Act 2024* (PRIS Act) and associated Western Australian Information Commissioner Privacy Guidelines. It covers identifying, containing, assessing, managing information breaches as well as notifying those affected by them.

It also covers shared information breaches under Part 3 Division 6 of the PRIS Act which occur in the context of the responsible sharing of information facilitated by Information Sharing Agreements.

The primary reference for step-by-step guidance when responding to a suspected or confirmed notifiable information breach is DTMI's Information Breach Response Plan (IBRP). It contains detailed instructions, including specific actions, timelines, and escalation procedures.

This document is to be read together with the Information Breach Policy. DTMI makes these documents publicly available in accordance with s.73 of the PRIS Act and relevant Information Commissioner Privacy Guidelines.

2. Scope

This document applies to all Authorised Users, being individuals or entities who are granted permission, in accordance with applicable law, DTMI policies and procedures, and relevant contractual arrangements, to access, process, manage or otherwise handle DTMI information or information systems.

Authorised Users include, but are not limited to DTMI employees (permanent and temporary).

It applies to all forms of personal information, whether recorded or not, including information that is held or controlled by DTMI, whether digital, physical, or verbal.

The mandatory notification and reporting scheme for information breaches under the PRIS Act commencement is on 1 January 2027.

3. Definitions and terms

Key terms used in this document are defined in the table below.

Term	Definition
Authorised User	An Authorised User is any individual or entity granted permission to access DTMI information systems and assets, including: • DTMI staff: Permanent and temporary employees, contractors, volunteers, interns, and trainees.

Term	Definition
	• Service partners: Agents, consultants, and organisations authorised to administer, develop, manage, or support DTMI information systems and assets. • Third-party providers: Suppliers, vendors, and hosted or managed service providers engaged by DTMI. An Authorised User is authorised only to the extent permitted by applicable law, DTMI policies and procedures, contractual arrangements, and the Information Privacy Principles under the PRIS Act. Access to, or use or disclosure of, information by an Authorised User outside that scope may constitute unauthorised access or unauthorised disclosure and an information breach for the purposes of this Procedure.
Assessed shared information breach	A shared information breach that has been assessed and determined to have occurred, or in respect of which there are reasonable grounds to believe that it has occurred. Source: section 192(4) PRIS Act
Assessed notifiable information breach	Either what an assessment determines to be a notifiable information breach, or what an assessment determines there are reasonable grounds to believe is a notifiable information breach. Source: section 61(3) PRIS Act
Chief Data Officer	A senior executive officer appointed under the *Public Sector Management Act 1994* Part 3 in an information sharing Department in accordance with section 198 of the PRIS Act. The CDO is responsible for building the capability of public entities to share information in accordance with the PRIS Act including information sharing between Western Australian public entities, external entities and across jurisdictions. The CDO monitors the use of information sharing agreements under the PRIS Act, provide advice on responsible information sharing, and issues guidance and guidelines to support lawful and effective information sharing practices.
Cyber security incident	A single or series of unwanted or unexpected event(s) that impact the confidentiality, integrity or availability of a network or system or the information that it stores, processes, or communicates. Source: WA Whole of Government Cyber Security Incident Coordination Framework (WA CSICF)
External entity	(a) is any of the following — (i) an agency or instrumentality of the Commonwealth, another State or a Territory; (ii) a contracted service provider; (iii) an Aboriginal community controlled organisation; (iv) a person or body that provides or promotes social services as defined in the *Children and Community Services Act 2004* section 3; (v) a higher education provider, as defined in the *Tertiary Education Quality and Standards Agency Act 2011* (Commonwealth) section 5,

Term	Definition
	that is registered in the "Australian University" provider category under that Act; (vi) a body that carries out health-related research; (vii) any other body, or the holder of any other office, that is prescribed by the regulations; but (b) does not include a public entity. Source: sections 4, 156(2) PRIS Act
Health information	(a) Personal information that relates to — (i) the health (at any time) of an individual; or (ii) the disability (at any time) of an individual; or (iii) an individual's expressed wishes about the future provision of health services to the individual; or (iv) a health service provided, or to be provided, to an individual. or (b) other personal information collected to provide, or in providing a health service Source: section 4 PRIS Act
Information breach	Unauthorised access to, or unauthorised disclosure of, information; or loss of information. Source: section 4 PRIS Act
IBRP	An information breach response plan. A detailed practical framework that sets out the steps the IBR team and Authorised Users must follow when an information breach is suspected, detected or reported. The plan guides DTMI in swiftly containing and assessing breaches, mitigating actual or potential, and ensures timely notification of relevant internal and external notifying stakeholders.
IBR team	DTMI's information breach response team. The IBR team typically includes representatives from Information Governance, Legal and Legislative Services, Cyber Security (if relevant), the affected DTMI business unit, Strategic Communications, and other specialists as needed.
Information Commissioner	The person appointed as Information Commissioner under section 5(2) of the *Information Commissioner Act 2024* (WA).
Information Sharing Agreement (ISA)	A written agreement entered into in accordance with the PRIS Act that provides for: 1. the disclosure for a permitted purpose of government information by a public entity to: a. another public entity; or b. an external entity; and

Term	Definition
	2. the collection, holding, management and use of that information by that other entity for a permitted purpose; and 3. the relevant activity to be carried out for that permitted purpose using the information. The agreement documents the authorised sharing of information, including: • What information is being shared; • Under what circumstances; • With whom and for what purpose; • How the information sharing will be implemented; and • The controls and mechanisms that ensure the personal information is being shared safely. The term of an agreement must not exceed 5 years. Source: sections 168, 170 PRIS Act
IPP entity	An IPP entity is a: (a) Minister; or (b) Parliamentary Secretary; or (c) public entity; or (d) contracted service provider. Source: sections 4, 14 PRIS Act
Information privacy principles	The Information privacy principles contained in Schedule 1 of the PRIS Act.
Likely to result	More probable than not, rather than merely possible.
Non-personal information	Information that is not personal information as defined in section 4 of the PRIS Act.
Notifiable information breach	Where personal information held by an IPP entity: • has been accessed or disclosed in an unauthorised manner, and a reasonable person would conclude that the access or disclosure is likely to result in serious harm to any individual to whom the information relates. • is lost in circumstances in which unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and if the access or disclosure of the information were to occur, a reasonable person would conclude that it would be likely to result in serious harm to any individual to whom the information relates. • either there is unauthorised access to, or unauthorised disclosure of, or loss, and the access, disclosure or loss occurs in circumstances set out in a notifiable information breach determination under section 60 by the Information Commissioner. Source: sections 4, 57 PRIS Act

Term	Definition
Permitted purpose	A purpose for which government information may be shared under an ISA, namely: • To inform or enable the making or implementation of government policy; • To inform or enable the design, management, delivery or evaluation of government programs and services; • To inform or enable research and development with clear and direct benefits to the public; • to inform or enable emergency management (including prevention of, preparedness for, response to, and recovery from, emergencies); and • an additional purpose prescribed by regulations. Information cannot be shared under an ISA fora purpose that relates to: • a law enforcement function of a law enforcement agency (other than a community policing function of the Police Force of Western Australia as prescribed by the regulations); or • determining whether a person has complied with a law or monitoring compliance with a law; or • national security; or • A primary purpose of obtaining commercial gain. Source: section159(3) PRIS Act
Personal information	(a) Information or an opinion, whether true or not, and whether recorded in a material form or not, that relates to an individual, whether living or dead, whose identity is apparent or can reasonably be ascertained from the information or opinion; and (b) including information of the following kinds to which paragraph (a) applies — (i) a name, date of birth or address; (ii) a unique identifier, online identifier or pseudonym; (iii) contact information; (iv) information that relates to an individual's location; (v) technical or behavioural information in relation to an individual's activities, preferences or identity; (vi) inferred information that relates to an individual, including predictions in relation to an individual's behaviour or preferences and profiles generated from aggregated information; (vii) information that relates to 1 or more features specific to the physical, physiological, genetic, mental, behavioural, economic, cultural or social identity of an individual. Source: section 4 PRIS Act
Privacy impact assessment (PIA)	Privacy impact assessment means a documented assessment of the privacy risks associated with a function, activity or relevant activity, including activities under a proposed information sharing agreement, that assesses the

Term	Definition
	likelihood and impact of any interference with privacy and identifies measures to manage, minimise or eliminate those impacts. Source: sections 4, 79(2), 80(2), 176(2) PRIS Act
Provider	The public entity that provided the shared information under an ISA to another public entity or an external entity. Source: section 168(2) PRIS Act
Public entity	A Western Australian government department or agency (including DTMI), a Senior Executive Service organisation under the *Public Sector Management Act 1994* (WA), the Western Australia Police Force, a judicial body, a local government, a statutory authority or government trading enterprise, or a body, or the holder of an office, established under a written law or by the Governor or a Minister, and includes any entity prescribed by the regulations. Source: section 6 PRIS Act
Recipient	The public entity or the external entity that collects, holds, manages and uses information disclosed to it under an ISA by another public entity Source: section 168(3) PRIS Act
Sensitive personal information	Personal information — (a) that relates to an individual's — (i) racial or ethnic origin; or (ii) gender identity, in a case where the individual's gender identity does not correspond with their designated sex at birth; or (iii) sexual orientation or practices; or (iv) political opinions; or (v) membership of a political association; or (vi) religious beliefs or affiliations; or (vii) philosophical beliefs; or (viii) membership of a professional or trade association; or (ix) membership of a trade union; or (x) criminal record; or (b) that is health information; or (c) that is genetic or genomic information (other than health information); or (d) that is biometric information; or (e) from which information of a kind referred to in any of paragraphs (a) to (d) can reasonably be inferred; Source: section 4 PRIS Act
Serious harm	Where the harm arising from the information breach has, or may, result in a real and substantial detrimental effect on an individual. Harm to an individual includes: • physical harm;

Term	Definition
	• economic, financial or material harm; • emotional or psychological harm; • reputational harm; and • other forms of serious harm that a reasonable person would identify as a possible outcome of the information breach.
Shared information	Government information (whether personal or non-personal) disclosed by DTMI to another public entity or an authorised external entity under an ISA made in accordance with Part 3, Division 4 of the PRIS Act.
Shared information breach	Where — (a) information has been disclosed to a recipient under an information sharing agreement; and (b) either — (i) an information breach occurs in relation to that information held by the recipient; or (ii) an event prescribed by the regulations in the PRIS Act occurs in relation to that information held by the recipient. Source: section 4, 191 PRIS Act
Suspected notifiable information breach	An information breach that has been identified but has not yet been assessed to determine whether it is likely to result in serious harm to any affected individual.
WA Whole of Government Cyber Security Incident Coordination Framework (WA WoG CSICF)	WA's whole-of-government process for cyber incident management and response. The WA CSICF establishes: • principles and priorities to guide decision making in the management of cyber security incidents; • roles and responsibilities for agencies, managed service providers, the Office of Digital Government, WA Police Force, the Directors General Technology, Innovation and Science Council (formerly the Directors General ICT Council), and RiskCover (cyber security insurance provider); and • requirements for reporting a cyber security incident, incident declarations, support to Ministers and the release of public information. Source: WA CSICF

4. Roles and Responsibilities

The following table lists the key roles and responsibilities of DTMI officers and other Authorised Users in the event of a suspected or confirmed notifiable information breach.

Role	Responsibilities
Director General	• Holds the ultimate accountability for ensuring that DTMI complies with the PRIS legislation. • Oversees the implementation of policies and procedures related to information security and information breach management. • In the event of a breach, makes high-level decisions and ensures that appropriate actions are taken to mitigate the impact and prevent future occurrences. • May delegate any powers, functions or responsibilities under this Procedure to the Deputy Director General and/or members of the Corporate Executive, as appropriate, while retaining ultimate accountability.
Corporate Executive (led by the Managing Director)	• Support the Director General in the strategic management of information security. • Approve and endorse policies, allocate resources, and ensure that DTMI's information protection measures are aligned with its overall objectives. • During an information breach, collaborate with other key stakeholders to manage the response and recovery efforts.
IBR team	• Carries out the procedures set out in this document and the undertakes the responsibilities specified in the information breach response plan in the event of an information breach.
Chief Information Officer	• Holds executive accountability for DTMI's information and cyber security capability, including preparedness for and response to information breaches. • Provides strategic oversight of technical containment and remediation activities undertaken by ICT, cyber security and service providers. • Ensures that appropriate resources, systems and controls are in place to support effective breach response and recovery. • Endorses major remediation actions and security improvements arising from information breach outcomes and post-incident reviews.
Director Information Governance	• Leads DTMI's information governance and privacy compliance, including oversight of PRIS Act obligations. • Coordinates and leads the information breach assessment process, including determining whether a breach is a suspected or assessed notifiable information breach. • Convenes and manages the Information Breach Response (IBR) team, ensuring timely assessment, documentation, escalation and notification where required. • Oversees and coordinates post-incident reviews for information breaches, supporting the relevant Director/Manager to identify

Role	Responsibilities
	root causes, governance or control gaps, and to develop recommended preventative measures. • Works with business owners and the CIO to ensure lessons learned are embedded into policies, procedures, training and assurance activities.
PRIS officer	• Ensures that DTMI complies with the PRIS legislation. • Develops and implements policies related to information protection and privacy, conducts training and awareness programs, and monitors compliance. • During an information breach, the PRIS officer assesses the impact on individuals' privacy, coordinates with the Information Commissioner, and in collaboration with the Strategic Communications team ensures that affected individuals are informed and supported.
Legal and Legislative Services	• Provide legal advice and support in relation to information breach assessment and response, including advice on statutory obligations under PRIS Act, legal risk and notification requirements. • In the event of an information breach, provide advice on legal and regulatory implications, manages or co-ordinates any legal proceedings, complaints or regulatory engagement arising from the breach and assists with the interpretation of applicable legislative requirements.
Strategic Communications and Engagement	• Manage all communications during and after an information breach including developing and executing the communication plan, serving as the primary contact for stakeholders and media. • Ensure timely and accurate information flow, safeguard DTMI’s reputation, and participate in post-incident reviews to improve future strategies.
Directors and Line Managers	• Implement information governance policies and procedures within their respective areas. • Ensure that their teams are aware of and comply with information protection measures. • During an information breach, coordinate with the IBR team to manage the response, support affected individuals, and implement corrective actions. • Conduct a post-incident review, prepare and submit a formal report to the IBR team for consideration and action.
Authorised Users	• Play a critical role in maintaining effective information governance and preventing, detecting and responding to information breaches. • Must comply with DTMI's policies and procedures, immediately report any actual or suspected information breaches or any suspicious activities, and participate in required training programs. • In the event of an information breach, cooperate with response and investigation activities, provide relevant information, and support containment, remediation and recovery actions.

5. Notifiable information breaches

For the purposes of Part 2 Division 6 of the PRIS Act, an information breach occurs when personal information, whether in digital or physical form held by DTMI is subject to unauthorised access, unauthorised disclosure or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure.

Such breaches are not confined to disclosure of personal information outside DTMI. For example, unauthorised access to personal information by an Authorised User, or unauthorised sharing of personal information between Authorised Users within DTMI may also amount to an information breach as it is inconsistent with the Information Privacy Principles in Schedule 1 of the PRIS Act.

An information breach may occur as the result of malicious action, systems failure, human error, or the loss of information. It may also occur because of a misunderstanding or misconception about whether a particular act or practice is permitted by the Information Privacy Principles including other legislative or policy requirements.

5.1 Examples

Examples of information breaches include:

- **Human error**
  - A letter or email is sent to the wrong recipient.
  - Information is accessed without appropriate authorisation.
  - An Authorised User fails to adhere to information security requirements, for example leaving information unattended, sharing password and login information, or ignoring confidentiality obligations.
- **Malicious or criminal attack**
  - Cyber security incidents such as ransomware attacks, malware, hacking, phishing scams and brute force access attempts resulting in access to or theft of personal information.
  - Social engineering or impersonation leading to inappropriate disclosure of personal information.
- **Insider threats**
  - Authorised Users using their valid credentials to access or disclose personal information outside the scope of their duties or permissions.
- **System failure**
  - Weak security.
  - Software bugs that expose personal information.
  - Poor vulnerability management, for example, failure to apply security patches leading to exploitation.
- **Physical theft of loss**
  - Theft of a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information.
  - Paper records with sensitive data being lost or misplaced.

6. Responding to and reporting on an information breach

There are five key steps in responding to a suspected notifiable information breach:

1. **Initial reporting and triage**

2. **Contain**
3. **Assess and mitigate**
4. **Notify**
5. **Review**

The last four steps are the focus of the IBRP and should be carried out concurrently where possible. The last step aims to provide recommendations for prevention strategies.

The following sections provide an overview of each step in the process. **Figure 1** provides an illustration of the typical process steps which DTMI Authorised Users must follow when identifying and reporting breaches of both minor and significant nature.

6.1 Initial detection and triage

A suspected notifiable information breach may be discovered by any DTMI Authorised User, or an Authorised User may be alerted to a breach by another party or system.

When an Authorised User suspects an information breach, they must immediately notify:

- their line manager and/or director; and
- Business Information Systems (BIS) and the PRIS officer by logging a ticket in ServiceNow – Report an Incident on DTMI's intranet (Transporta). For illustration, the notification form in **Appendix 1** shows the details required when reporting a suspected breach.

The Authorised User should provide as much information as possible about the context of the suspected breach, including:

- the time and date that it was discovered;
- the type of information involved;
- its cause; and
- its extent.

Where an Authorised User can take steps to contain the suspected notifiable information breach, they must do so as soon as possible. Examples include:

- trying to recall an email sent to an incorrect recipient;
- requesting the person outside DTMI who incorrectly received the information to permanently delete it; and
- taking steps to withhold or remove a document that was incorrectly published on DTMI's website.

Authorised Users must retain documents related to the breach. They must not be deleted as that may impede any later assessment.

The Director Information Governance leads and coordinates the assessment to determine whether an information breach may have occurred, with input from the relevant line manager or Director of the affected DTMI business unit. Where there are reasonable grounds to suspect that a breach has occurred, the Director Information Governance must immediately convene the IBR team.

All information provided by the Authorised User who first identified the breach, and the initial assessment must be documented as it may be relevant to the assessment.

6.2 Contain

Containing the information breach is DTMI's priority.

Authorised Users must take all possible steps to contain the information breach and minimise any resulting damage. This may include locking down of a physical location and disabling remote access.

6.3 Assess and mitigate

Once the breach has been contained, the IBR team (and the Director Information Governance in particular) assesses its impact. The Director Information Governance confirms compliance with the assessment and notification timeframes under the PRIS Act and escalates the matter to the Director General (or delegate) as soon as practicable where those timeframes are at risk of not being met.

The key issue to consider is whether there has been a notifiable information breach. These are breaches that involve personal information and that a reasonable person would conclude are likely to result in serious harm to any individual to whom the information relates.

In determining whether 'serious harm' is 'likely to result' to an individual to whom the information relates, they consider the following matters:

- the type of personal information accessed, disclosed or lost, and whether a combination of types of personal information might lead to increased risk;
- the level of sensitivity of the personal information accessed, disclosed or lost;
- the amount of time the personal information was exposed or accessible, including the amount of time personal information was exposed prior to DTMI discovering the information breach;
- the circumstances of the individuals affected and their vulnerability or susceptibility to harm (that is, if any individuals are at heightened risk of harm or have decreased capacity to protect themselves from harm);
- the likelihood that the persons involved (those who accessed the information) have or had the intention of causing harm, or could or did circumvent security measures protecting the information;
- the circumstances in which the information breach occurred; and
- actions taken by DTMI to reduce the risk of harm following the information breach.

Assessment of the likelihood of serious harm arising from an information breach is an objective test.

If there is a suspected notifiable information breach, the IBR team will:

- immediately take all reasonable steps to contain the suspected notifiable information breach; and
- as soon as reasonably practicable and no later than 30 days after the day on which the reasonable suspicion is formed —
    - conduct an assessment for the purposes of determining whether a notifiable information breach has occurred or there are reasonable grounds to believe that a notifiable information breach has occurred; and
    - prepare a written report on the assessment;

  and;
- take all reasonable steps to mitigate any harm caused by the suspected notifiable information breach.

Where the assessment determines that the breach is a notifiable information breach, or that there are reasonable grounds to believe it is a notifiable information breach, the breach becomes an assessed notifiable information breach and the notification requirements under the PRIS Act apply, including notification to the Information Commissioner.

In preparing its report on the assessment, the IBR team will consider any relevant Information Commissioner guidelines.

The IBR team may seek an extension of time from the Commissioner in which any notices may be provided.

The IBR team implements mitigation measures to reduce risk and prevent further misuse of compromised information. These measures may include strengthening security controls, removing exposed data from public sources, and working with third parties such as identity issuers or financial institutions to limit potential harm.

The PRIS officer must update the DTMI Information Breach Register in light of the above.

6.4 Notify

If the IBR team confirms that a notifiable information breach has occurred then it is considered an assessed notifiable information breach and as soon as is practicable the PRIS officer must notify:

- the Information Commissioner;
- other IPP entities or relevant Australian or international organisations, as applicable; and
- affected individuals.

The purpose of notification is to help mitigate potential harm.

In cases where the breach does not meet the threshold for a notifiable information breach, the IBR team may still decide to notify individuals or organisations if the nature of the information, the risk of harm, or repeated issues warrant proactive communication.

The timing and method of notification depends on the scale and circumstances of the breach. Affected individuals may be notified:

- directly, for example, by telephone, email, letter, or in person; and
- indirectly, such as through public notices or website announcements, where direct contact details are unavailable or where direct notification could cause further harm.

Notifications will include key details such as:

- entity and contact details;
- the date and nature of the breach;
- the type of personal information involved;
- actions taken to contain the breach; and
- recommended steps for individuals to protect themselves.

In addition to notifying affected individuals and the Information Commissioner, the IBR team will consider whether contractual, legislative, or administrative obligations require engagement with external stakeholders. Depending on the circumstances, these may include:

- law enforcement agencies;
- cyber security authorities;
- regulatory bodies;
- financial institutions; and
- identity protection services.

These actions ensure that all relevant parties are informed and that appropriate measures are taken to reduce the risk of further harm.

Where multiple IPP entities are involved, the IBR team is responsible for ensuring that DTMI collaborates with all relevant parties to ensure a coordinated response and determine whether external notifications or communications are required.

Under the PRIS Act exemptions to the notification requirement can apply.

6.5 Review

Following containment, assessment, and notification, the IBR team undertakes a review of the circumstances surrounding the assessed notification information breach to identify its causes and determine measures to prevent recurrence. Depending on the nature of the breach, this step may be integrated with earlier stages of assessment and mitigation.

- The Director Information Governance oversees and coordinates the post-incident review.
- The Director/Manager of the DTMI business unit where the breach originated prepares the post-incident review report using the 'Information Breach Assessment and Resolution Form' in **Appendix 2** and submits it to the IBR team for consideration and action.

Preventative measures may include:

- reviewing DTMI's IT systems and implementing remedial actions;
- conducting security audits of physical and technical controls;
- updating policies and procedures;
- improving Authorised User training; and
- reassessing contractual obligations with service providers.

Recommendations arising from the review must be approved by the Chief Information Officer and/or relevant Corporate Executive member and recorded in DTMI's electronic recordkeeping system. The IBR team decides whether a matter is sufficiently significant to warrant its being reported to the Director Governance and Audit within the Office of the Director General. Examples of significant matters may include breaches involving a large number of individuals or sensitive personal information, systemic or repeated control failures, or incidents with material regulatory, reputational, financial or operational impact for DTMI.

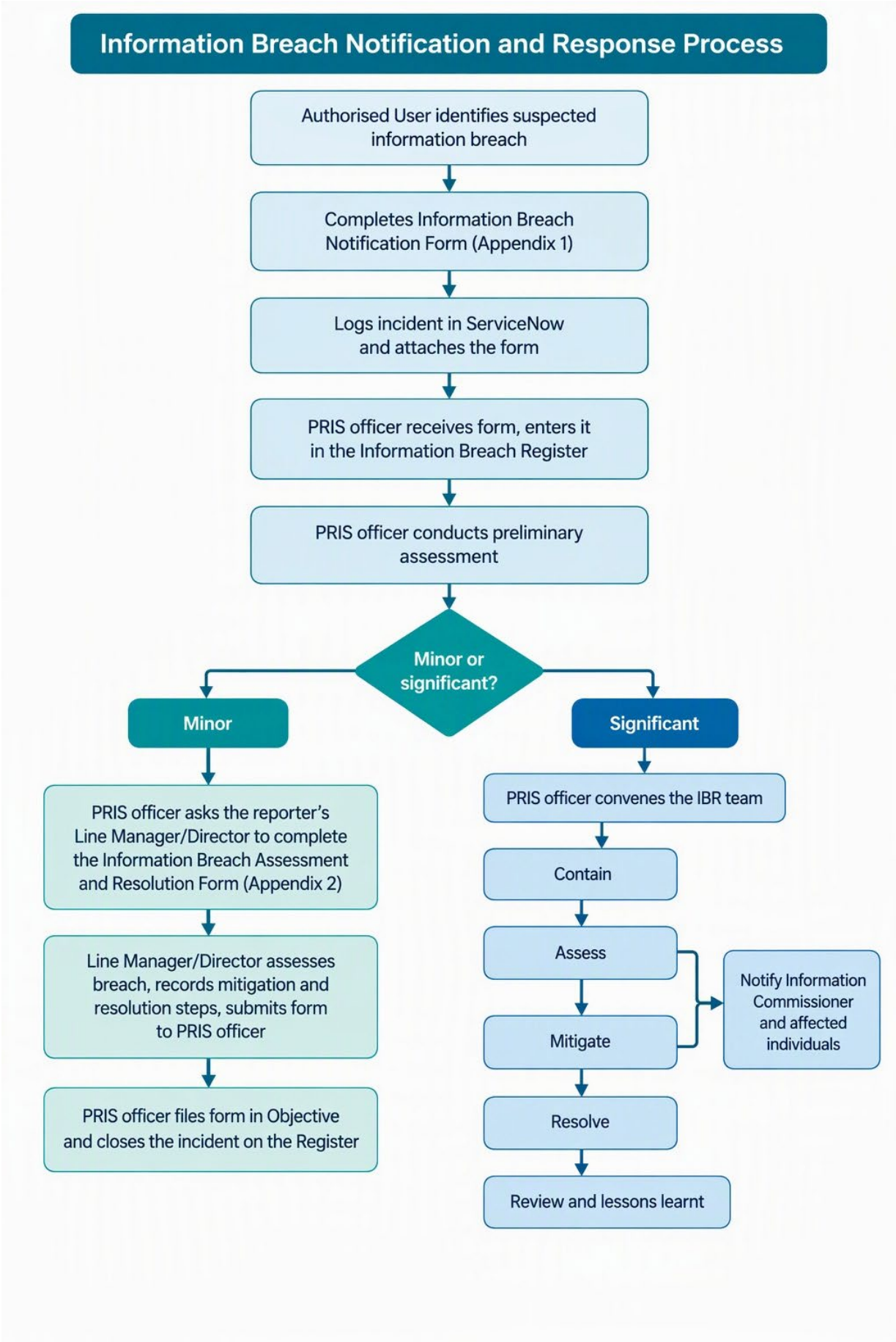

Figure 1. Basic flowchart illustration of the general process steps involved in dealing with minor (non-notifiable) or significant (notifiable) breaches.

7. Shared information breaches – Overview

Part 3 Division 6 of the PRIS Act provides for the management of information breaches involving shared information.

A shared information breach occurs if:

- information has been disclosed to a recipient (an IPP entity or an external entity) by a provider under an information sharing agreement (ISA); and
- either —
  - an information breach occurs in relation to that information held by the recipient; or
  - an event prescribed by the regulations occurs in relation to that information held by the recipient.

Under the PRIS Act, DTMI may act either as a:

- provider sharing DTMI information with other IPP entities or external entities under an ISA; or
- recipient when receiving information of other IPP entities under an ISA.

If a recipient under an ISA forms a reasonable suspicion that a shared information breach has occurred, the recipient must:

- immediately take all reasonable steps to contain the suspected shared information breach and notify the provider as soon as practicable;
- as soon as reasonably practicable (but within 30 days after the day of forming a suspicion) conduct an assessment to determine whether a shared information breach has occurred or there are reasonable grounds to believe that a shared information breach has occurred;
- prepare a written report of the assessment (having regard to any Chief Data Officer (CDO) guidelines about assessments) and give the provider a copy as soon as the report is completed; and
- take all reasonable steps to mitigate the harm caused by the suspected shared information breach.

The recipient must notify the CDO and the information provider of an assessed shared information breach, in accordance with Part 3 Division 6 of the PRIS Act.

- In circumstances where the shared information breach meets the definition of a notifiable information breach involving personal information, the provider must notify the Information Commissioner and affected individuals in accordance with Part 2 Division 6 of the PRIS Act.

7.1 Managing shared information breaches – Additional information

To assist with the procedures required when managing shared information breaches, **Appendix 3** provides practical checklists that complement the procedures set out in this document:

1. **Process for managing shared information breaches under an ISA:** the key actions required when a shared information breach occurs, including notification, containment, assessment, and mitigation.
2. **Responsibilities:** the obligations of DTMI as a provider or a recipient under an ISA, ensuring clarity on who does what during a breach response.
3. **Notifications to regulators:** the mandatory reporting requirements to the CDO and the Information Commissioner, including triggers, responsible parties, and timeframes.

4. **Essential ISA clauses for managing shared information breaches:** the critical contractual provisions that must be included in ISAs to ensure compliance and effective breach management.

8. Recordkeeping

8.1 Document creation

An Authorised User who creates a document during the information breach response process must record it in the relevant folder in Objective. That includes all assessment reports, notifications, and communications from the Information Commissioner and/or the CDO.

8.2 Register of Information Breaches

DTMI maintains a register of information breaches as required by section 74 of the PRIS Act. The PRIS officer is responsible for maintaining the register and ensuring that it includes updated logs of all breaches for audit and reporting purposes.

Amongst other information regarding each notifiable information breach, DTMI's register will include the following details:

1. Whether the unauthorised access, unauthorised disclosure or loss of personal information is likely to result in serious harm, or if a notifiable information breach determination has been made by the Information Commissioner.
2. Whether the breach was reported to the Information Commissioner, including date of notification.
3. Whether affected individuals were notified of the breach, including their names if notified (including whether a listed exception to the notification requirement applies due to reasons listed under sections 64-68 of the PRIS Act).
4. Details of actions taken to contain and mitigate the harm caused by the breach.
5. Details of measures taken to prevent future breaches of the same kind.
6. The estimated cost of the breach to DTMI.

Additionally, the register includes:

- records of suspected notifiable information breaches that were not found to be assessed notifiable information breaches.
- shared information breaches.

The PRIS officer is responsible for maintaining DTMI's register of information breaches and ensuring that it includes updated logs of all breaches for audit and reporting purposes.

8.3 Annual Report

DTMI will include in its annual report the information required by section 75 of the PRIS Act concerning the year's assessed notifiable information breaches. Information included in the annual report will be presented in an aggregated or de-identified form where appropriate to minimise further privacy impacts.

9. Review and continuous improvement

This document is to be reviewed every 2 years or after any breach assessed as a notifiable information breach.

10.Communication Strategy

The Director Strategic Communications and Engagement is responsible for all communications issued under this document.

11.Related Information

Legislation

- *Privacy and Responsible Information Sharing Act 2024*
- *Privacy and Responsible Information Sharing (General) Regulations 2026*
- *Privacy and Responsible Information Sharing (Information Sharing) Regulations 2025*
- *Privacy and Responsible Information Sharing (Privacy) Regulations 2025*
- *Freedom of Information Act 1992*
- *Freedom of Information Regulations 1993*
- *Information Commissioner Act 2024*
- *Information Commissioner Regulations 2025*
- *State Records Act 2000*
- *State Records Regulations 2025*
- *Public Sector Management Act 1994*
- *Privacy Act 1998 (Cth)*

Policies and Procedures

- Privacy Policy
- Information Breach Policy
- Information Breach Response Plan (internal)
- Managing Privacy Complaints Procedure (internal)

Forms

- Information Breach Notification Form [internal]
- Information Breach Notification Form [public]
- Information Breach Assessment and Resolution Form [internal]

Other references

- Register of information breaches (internal, restricted)

Appendix 1. Information Breach Notification Form

For **DTMI Authorised Users:** complete this form and log an incident via ServiceNow – Report an incident. Attach the completed form to your log.

Members of the public or external parties: Use a stand-alone, adapted version of this form to report suspected information breaches and email it to privacy@transport.wa.gov.au.

DTMI will use the information to respond to the suspected information breach in accordance with the *Privacy and Responsible Information Sharing Act 2024* (WA).

Details of the Authorised User reporting the breach incident				
Full name				
Position title		Location and Business Unit		
E-mail		Contact phone number		
Line Manager		Manager Notified	☐ Yes	☐ No

Details of the breach incident			
Location	*DTMI Business Unit where the breach occurred*		
Date the breach was identified *Click or tap to enter a date.*	Date when first became aware of the breach *Click or tap to enter a date.*	Date (if known) when the breach occurred, or best estimate *Click or tap to enter a date.*	Time (if known) when the breach occurred *Enter time*
What is the Information accessed?	☐ Personal information, including sensitive personal information	☐ Non-personal information	☐ Both
Information asset details (as referenced in DTMI's Information Asset Register)	Application System	Application System Owner contacted?	Click or tap to enter a date.
	Type of Business Process *E.g.: Customer data, Investigations, Employee*	Business Process Owner contacted?	Click or tap to enter a date.
Information Breach method. *Multiple boxes can be selected.*	☐ Human error	*E.g., sending data to the wrong person or losing a device*	
	☐ Insider threat	*E.g., misuse or theft by staff or contractors*	
	☐ Malicious attack	*Such as phishing, malware, or credential theft*	
	☐ System failure	*Such as weak security or poor incident response*	
	☐ Physical breach	*E.g., theft of documents or unauthorised access to secure areas*	
	☐ All Apply		

	☐ Other/ Unknown	

Description of the breach – Provide a brief and factual information only to inform the assessment	
What happened?	*Example: Personal Information about an individual was accessed in TRELIS and provided to a relative.*
Description of the specific information accessed	*Example: body worn camera recordings.*
Who accessed or received the information?	*Accessed by and/or provided to who?*
Was the breach intentional?	*Unauthorised, Intentional or unintentional?*
Describe what information was affected.	*Include details such as the volume affected, identifiability, and whether the information related to an individual(s) or corporate records. E.g. A report listing details of 100 individuals in TRELIS; details of the Information Sharing Agreement under which the affected information was shared.*
Who/What caused it?	*Initial known or assumed cause of the breach. This may differ to the confirmed cause after further investigation.*
Who has been notified or has knowledge of the incident?	*List individuals or parties notified.*
What immediate containment actions were taken, if any?	*E.g. email recalled, access disabled, system isolated etc.*
In your opinion, do you believe that the breach is likely to cause serious harm to an individual?	*Explain rationale.*

Appendix 2. Information Breach Assessment and Resolution Form

To be completed by the Director/Manager of the DTMI business unit where the breach originated and provided to the PRIS officer via ServiceNow – Report an incident.

Details of the individual undertaking the assessment of the breach incident.			
Full name			
Position title		Location and Business Unit	
E-mail		Phone number	

Assessment			
Date received		Date commenced	
Potential breach of discipline/code of conduct	☐ Yes ☐ No	*If yes, immediately notify the Executive Director People and Culture, and comply with further instructions.*	
Cyber security breach?	☐ Yes ☐ No	*If yes, immediately contact DTMI IT Service desk: 16999 or 1800216222 or Report an Incident on TRANSPORTA via ServiceNow and comply with their instructions.*	
The breach is an assessed notifiable information breach	☐ Yes ☐ No	Provide reasons that justify the assessment.	
The breach is likely to cause serious harm to an individual	☐ Yes ☐ No	Explain the basis on which this conclusion is made.	
Who is affected by the information breach?	*E.g. Authorised Users, members of the public, other government agencies, third party stakeholders.* *The assessment may include reviewing whether individuals/organisations have been affected by the breach.*		
Who has been notified of the breach?	*Record who and date notified.*		
What immediate actions were taken to contain the breach?	*What was done to manage the risk of further damage/harm?* • *Has the information been recovered?* • *Security measures taken.*		
What caused it? Identify the causal factors and underlying causal circumstances.	*The assessment may include reviewing:* • *How did the current controls fail to mitigate the risk of breach?* • *Whether the breach occurred as part of a deliberate act or negligence.* • *Was it a one-off incident or does it expose a more systemic vulnerability?*		

Assessment	
What is the potential harm to the affected individuals or the organisation?	*Consider the level of sensitivity of the information and what possible use there is for the information. For example, could it be used for identity theft, threats to physical safety, financial loss, or damage to reputation?* *Is it official information that could result in damage to individuals, organisations or government if released* *Whether any individuals have personal circumstances which may put them at particular risk of harm.*
What controls were in place to mitigate the risk of this information breach?	*For example: Policy, Procedures, Restricted Access, Monitoring, Security etc.*

Review and Risk Management	
Is further investigation considered necessary and if so, how will this be undertaken?	*Will the breach need to be escalated or transferred to another authority?*
Risk Assessment. Refer to DTMI risk reference tables	*Consider: Individual harm, financial loss, service interruption, reputational damage. Assess:* • *The likelihood and consequence should the breach recur.* • *The controls managing the risk.* • *Risk acceptance/tolerance.*
After looking at the DTMI risk reference tables, what is the level of risk for the most impacted category?	• *1 Insignificant* • *2 Minor* • *3 Moderate* • *4 Major* • *5 Catastrophic*
Mitigation Action Plan - What is required to prevent the breach from occurring again?	*The mitigation action plan may include:* • *Strengthening the current controls and any additional controls that have been developed/implemented.* • *Improving security and access.* • *Education and training.* • *Changing the environment or location.*
Are PRIS Act assessment and notification timeframes on track to be met?	*If at risk, specify:* • *Which timeframe(s) are at risk (assessment / notification)* • *Date and details of escalation to Director Information Governance / Director General (or delegate)* • *Any engagement with the Information Commissioner regarding extensions*

Assessment Status and Closure		
Assessment status	☐ Assessment ongoing	☐ Assessment complete

Notifications (if applicable)	☐ Information Commissioner notified (if required) ☐ Affected individuals notified (if required) ☐ Notifications not required *(explain basis for rationale)*
Mitigations actions	☐ Mitigation actions identified ☐ Mitigation actions assigned to responsible owner(s) ☐ Mitigation actions completed ☐ Ongoing mitigation actions *(provide details and expected completion date)*
Assessment closure	Assessment closed on: ___ / ___ / _____ Approved by: Name: _____ Position / Role: _____

On completion, please forward this form to the PRIS officer.

Appendix 3. Quick Reference Checklists: Shared Information Breaches

DTMI Authorised Users must use these checklists when responding to shared information breaches relating to:

- information disclosed under an ISA by DTMI to another IPP entity or an external entity; and/or
- information received by DTMI from another IPP entity.

They are designed to complement the procedures in this document and the IBRP, enabling Authorised Users and decision-makers to respond quickly and consistently when a shared information breach occurs.

Checklist 1: Actions required for Managing Shared Information Breaches under an ISA

Stage 1 – Actions on reasonable suspicion of a shared information breach

These actions apply as soon as a recipient forms reasonable grounds to suspect that a shared information breach may have occurred.

Key action	Description	Details Required
Contain the suspected breach	Take all reasonable steps to stop or limit further unauthorised access, disclosure or loss of shared information.	• Access disabled • Systems secured • Information retrieved or quarantined (where possible)
Notify the provider	Notify the provider's nominated ISA contact officer as soon as practicable after forming a reasonable suspicion.	• Date and time of notification • Description of suspected breach
Commence assessment	Begin assessment to determine whether a shared information breach has occurred or whether there are reasonable grounds to believe it has occurred.	• Date assessment commenced
Prepare assessment report	Prepare a written assessment report in accordance with the PRIS Act and any applicable CDO guidelines.	• Description of incident • Known or suspected cause • Information involved
Mitigate harm	Take all reasonable steps to mitigate any actual or potential harm arising from the suspected breach.	• Actions taken or planned
Record the incident	Record the suspected shared information breach in the recipient's Information Breach Register.	• Register entry completed

Stage 2 – Actions following completion of assessment

These actions apply once the assessment is completed and a determination has been made.

Key action	Description	Details Required
Determine assessment outcome	Determine whether an assessed shared information breach has occurred or whether there are reasonable grounds to believe it has occurred.	• Assessment outcome recorded
Provide assessment report to provider	Provide the provider with a copy of the completed assessment report as soon as practicable after completion.	• Date report provided
Notify the Chief Data Officer (if required)	Where an assessed shared information breach has occurred, notify the CDO in the approved form.	• Date and method of notification
Apply Part 2 notification requirements (if applicable)	Where the breach is also an assessed notifiable information breach involving personal information, notify the Information Commissioner and affected individuals in accordance with Part 2 Division 6 of the PRIS Act.	• Notifications completed / exemptions applied
Finalise records and reporting	Finalise assessment documentation and ensure registers and reporting records are updated.	• Register updated • Reports finalised

Checklist 2: DTMI's Responsibilities as a recipient/provider in the event of a shared information breach	
Role	**Responsibilities**

DTMI is a recipient	Upon becoming aware of a breach of shared information, DTMI must take the following actions:
	• Identify relevant ISA and clauses related to breach notification and contact officers.
	• Immediately take all reasonable steps to contain the suspected shared information breach.
	• As soon as practicable, or within 30 days of reasonably suspecting a breach:
	  ○ Investigate to determine if shared information has been compromised or if there are reasonable grounds to believe so.
	  ○ Prepare a written report detailing the assessment (follow any CDO Guidelines for conducting the assessment and the report).
	  ○ Take all reasonable steps to mitigate the harm caused.
	• As soon as practicable, notify the provider after reasonably suspecting a breach, as well as the outcome of the assessment and a copy of the report on that assessment.
	• As soon as practicable after determining that an assessed shared information breach has occurred or there are reasonable grounds to believe so, notify the

Checklist 2: DTMI's Responsibilities as a recipient/provider in the event of a shared information breach	
Role	**Responsibilities**
	CDO in writing of the breach. The notice must be in the approved form and include the following information: ○ The name and contact details of the recipient. ○ Details of the relevant information sharing agreement. ○ The name and contact details of the provider who disclosed the shared information involved in the breach. ○ The time (if known) and date on which the breach occurred. ○ A description of the breach and how it occurred. ○ Whether the breach involved unauthorised access, disclosure, or loss of shared information. ○ The kind of information involved, including whether it is personal information. ○ The period of time of the unauthorised access or disclosure (if applicable). ○ Steps taken or to be taken by the recipient to contain and mitigate the harm caused by the breach. ○ Any other information required by the approved form. ○ The kind of information involved in the shared information breach, including whether any of the information is personal information.
DTMI is a provider	If the information breach involves shared information held by a recipient that is a non-IPP entity, and the breach is an assessed notifiable information breach (i.e., serious information breach involving personal information) DTMI must regard the breach as though it is a breach involving personal information held by the provider. In this case, DTMI must treat the incident under the notifiable information breach provisions in Part 2 Division 6 of the PRIS Act (applicable to breaches involving personal information). This responsibility relates to statutory assessment, notification and mitigation obligations and does not determine fault or contractual liability. What this means is that DTMI, as an IPP entity, must treat the incident as a notifiable information breach, even though the originating breach occurred in the hands of a non-IPP recipient. DTMI is responsible for the following: • Conduct an assessment following the same steps as if the breach occurred internally: for example, assess the seriousness of the breach and the individuals affected. • Take steps to contain and mitigate the harm caused. • Notify: ○ the individuals affected in line with section 62 of the PRIS Act. ○ The Information Commissioner in line with section 63 of the PRIS Act, in addition to which it also must provide: ▪ the recipient's name and contact details; and

Checklist 2: DTMI's Responsibilities as a recipient/provider in the event of a shared information breach	
Role	**Responsibilities**
	▪ a description of the steps taken (or to be taken) by the recipient to contain and mitigate the harm. • Engage the recipient for any information and assistance needed to meet the reporting obligations under the relevant notifiable breach provisions. For details pertaining to the Information Commissioner notification requirements, refer to the Information Breach Procedures and the IBRP.

Checklist 3: Notifications to regulators			
Regulator	**Trigger**	**Responsible Party**	**Timeframe**
Chief Data Officer	Breach of shared information held by the recipient	Recipient	As soon as practicable after assessment (s.193)
Information Commissioner	Breach of shared personal information that is notifiable and the recipient is a non-IPP entity	Provider	As soon as practicable after assessment (s.62 with reference to s.194)

Checklist 4: Essential ISA clauses for managing shared information breaches	
Clause	**Purpose**
Prompt notification of breaches	Require the recipient to notify DTMI within 1 or 2 working days (s.192(3) of the PRIS Act).
Contact officers	Nominate an ISA contact person for each party for notification and communication purposes.
Shared breach response plan	Define a shared breach response plan, including: • Investigation protocols • Mitigation obligations • DTMI's rights to suspend or terminate the agreement.
Cooperation	Require cooperation with: • DTMI's internal breach assessment • Notifications to the CDO (s.193 of the Act).
Secure destruction/return	Specify obligations around destruction or secure return of information if necessary.
Consequences for non-compliance	Set out consequences for contravening the requirements regarding: • The assessment, containment, mitigation and notification to the provider under section 192 of the PRIS Act - mandatory requirement.

Checklist 4: Essential ISA clauses for managing shared information breaches	
Clause	**Purpose**
	• The notification requirement under section 193 of the PRIS Act (CDO) and under section 62 with reference to section 194 of the PRIS Act (the Information Commissioner) - mandatory requirement.