



Privacy Threshold Assessment

Version 5.0

Last update: 26 June 2025

OFFICIAL: Sensitive – Legal Privilege

LEGAL SERVICES DIVISION

Contents

When should this form be used?.....	3
Part 1: Project details.....	4
Part 2: Project description.....	6
Part 2a: Customer safety.....	8
Part 3: The Information	10
Part 4: Risk assessment.....	21
Part 5: Determination and recommendations	23
Appendix A.....	30
Appendix B	31
Appendix C	32

OFFICIAL: Sensitive – Legal Privilege

Privacy Threshold Assessment

When should this form be used?

Services Australia's Operational Privacy Policy requires a Privacy Threshold Assessment (PTA) be completed for:

1. all new projects¹; and
2. any other activities

which involve changes to the way the agency manages (i.e. collects, uses, stores, exchanges or discloses) any customer or staff personal information.²

'Projects' is intended to loosely describe any activities and initiatives undertaken by the agency, as well as programs/services delivered by the agency. Projects can include:

- new policy proposals
- new or amended legislation or delegated legislation
- program design and delivery
- new or changed programs or activities
- new ways of interacting with, or providing services to, customers · technology solutions to support service delivery, business processes and workflow management · alpha, beta, pilot and proof of concept (PoC) phases of these activities; and · market testing and procurements for products and services that will support service delivery or business processes
- implementing IT systems or databases or increasing the number of users of those systems
- new or changed methods or procedures for service delivery or information handling
- implementing artificial intelligence technologies, including automated decision-making processes
- restructures or changes to business-as-usual activities.³

Before completing this form, ensure you have necessary approvals from the right business areas to seek this legal advice as indicated below.

If you are from a Group other than:

1. Program Design Group and your project relates to program legislation or a program managed by the Program Design Group, you must also include written agreement from the National Manager (or above) of the relevant program in the Program Design Group.
2. Strategy Design Excellence and project relates to AI or automation, you must also include written agreement from the National Manager (or above) of the relevant Strategy Design Excellence area.

Once the necessary approvals have been obtained, please email a completed copy of the PTA form to one of the following Teams:

For all projects related to myGov and Digital ID: **s47E(d)** [@servicesaustralia.gov.au](mailto:s47E(d)@servicesaustralia.gov.au)

For any other projects: **s47E(d)** [@servicesaustralia.gov.au](mailto:s47E(d)@servicesaustralia.gov.au)

For more information about Privacy Threshold Assessments, please see **Appendix A**.

¹ See Appendix A for more information on what is considered a 'project'.

² See Appendix B for a description of personal, sensitive and protected (customer) information.

³ [What is a project](#)

servicesaustralia.gov.au

From: s22
To: s22
Cc: s22 ; s22 ; s22 ; s22 ; s22
Subject: Summary of final advice: LEX 65930 - s 42 s42
[SEC=OFFICIAL:Sensitive, ACCESS=Legal-Privilege]
Date: Tuesday, 27 January 2026 8:10:00 AM
Attachments: [image001.jpg](#)
[image002.png](#)
[image003.png](#)
[20260112 - LEX 65930 - s 42](#) [FINAL\).pdf](#)
[image004.png](#)

Dear s22

Thank you for chatting with me. As discussed, I have provided a summary of the advice below.

s42

s42

Kind regards,

s22

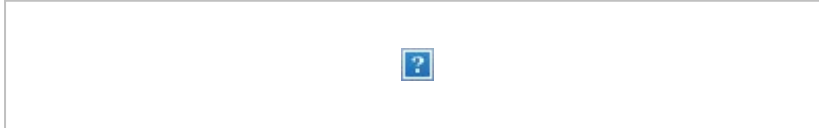
, Senior Government Lawyer

Privacy, Secrecy and Data Governance

Digital Delivery and Privacy Legal Branch, Legal Services Division



call me on [Teams](#) or by phone: s22



s22 (out of scope)

s22 (out of scope)

From: s22 <s22@servicesaustralia.gov.au>
Sent: Monday, 22 December 2025 5:17 PM
To: s22 s22@servicesaustralia.gov.au
Cc: s22 <s22@servicesaustralia.gov.au>; s22
<s22@servicesaustralia.gov.au>; s22
s22@servicesaustralia.gov.au>; s22

< [@servicesaustralia.gov.au](mailto:servicesaustralia.gov.au)>

Subject: RE: For review: LEX 65930 – **s 42**

[SEC=OFFICIAL:Sensitive, ACCESS=Legal-Privilege]

Hi **s22**

s42, s47C

s42, s47C

Kind regards,
s22

s22, Government Lawyer

call me on [Teams](#) or by phone: s22

Privacy, Secrecy and Data Governance | Legal Services Division



Services Australia acknowledges the Traditional Custodians of the lands we live on. We pay our respects to all Elders, past and present, of all Aboriginal and Torres Strait Islander nations.

Please note: This email and any attachments may contain information subject to legal professional privilege or information that is otherwise sensitive or confidential. If you are not the intended recipient of this email, you are prohibited from using or disseminating this communication. If you have received this communication in error please notify the sender immediately and permanently delete this email.

s22 (out of scope)



OFFICIAL: Sensitive
Fivecast ONYX User Guidelines
Intelligence and Investigations Branch
Version 1.3 July 2021

REVISION HISTORY

Version	Date	Created by	Comments
1.0	13/05/2021	TIFI Policy	User Guidelines
1.1	9/06/2021	TIFI Policy	Minor amendment to section 3
1.2	22/06/2021	TIFI Policy	Minor amendments to sections 3 and 9
1.3	1/07/2021	Operational Policy Team	Branch name changes & minor amendments to sections 3 and 9

Contents

1	Introduction.....	4
2	Open source information and social media	4
3	What is ONYX.....	4
4	Risks and issues	5
5	Relevant documents and instruments.....	5
6	Terms and conditions of use.....	6
7	How to complete a User Agreement	6
8	Roles and responsibilities	7
8.1	Users	7
8.2	Managers.....	7
8.3	Administrator	7
9	Access, use and storage of information.....	7
9.1	Key principles	7
9.2	Before undertaking searches	8
9.3	Undertaking searches.....	8
9.4	Explicit, highly sensitive or unlawful content.....	8
9.5	Documenting searches	8
9.6	Using findings	9
9.7	Storage of findings.....	9
9.8	Disclosing findings	9
10	Administration.....	10
10.1	Support and advice	10
10.2	Auditing.....	10

1 Introduction

These guidelines provide the Branch staff and managers with guidance and requirements for the use and oversight of ONYX software as part of intelligence and investigation activities.

These guidelines apply only to the use of ONYX in the context of these intelligence and investigation activities, but does not apply to any other tool or methods of sourcing information.

For the purposes of these guidelines:

- The word “must” denotes a requirement e.g., “Users must...” or “Users must not...”
- The terms “should” or “may wish to” denotes better practice e.g., “Users should...”
- The term “users” refers to analysts or investigators using ONYX as part of their intelligence and investigation activities.
- The term “case management system” refers to any Branch case management system.

2 Open source information and social media

Open source intelligence (OSINT) is information sourced from publically available sources.

Social media is online services or tools used to publish, share or discuss information. Examples are forums, blogs, wikis and social networking websites. These platforms allow individual users to upload, comment on and share content. Social media information is a form of OSINT.

Other forms of OSINT includes publically available data on websites, and data obtained from the use of geospatial tools.

3 What is ONYX

s47

s47, s37(2)(b)

s47, s37(2)(b)

4 Risks and issues

s37(2)(b), s47E(d)

5 Relevant documents and instruments

All usage of ONYX must be consistent with the following documents and instruments:

- The Australian Public Service Code of Conduct (APS Code). Relevant elements include APS Code requirements outlining that APS employees, in respect of their APS employment, must at all times behave honestly and with integrity, act with care and diligence, and use Commonwealth resources (which includes ONYX) in a proper manner and for a proper purpose.
- The agency Conduct and Behaviour Policy. Relevant sections include “Protecting information”. This section outlines requirements that agency employees must only access personal or protected information as part of their official duties, and when authorised to do so. It also notes that searching for, viewing, recording, using or disclosing personal or protected information other than in the performance of these official duties may constitute “unauthorised access”, which can result in APS Code breaches, other disciplinary action, and/or criminal prosecution being taken against employees found in breach.
- The Australian Privacy Principles (APPs). Relevant elements include APPs 3, 5, 6, 10 and 11, which regulate how the agency collects, uses and discloses personal and sensitive information.
- All confidentiality and secrecy provisions within social security, families, health, child support and disability services law relevant to the use and release of personal or protected information.
- All other relevant laws, policies and guidelines relating to the use, storage and dissemination of personal or protected information. This includes the Australian Government Investigation Standards, and the Protective Security Policy Framework (PSPF), which outlines requirements relating to security governance and information, personnel and physical security.
- User Agreements. Users must complete a User Agreement prior to using ONYX and whenever there is a significant change, update or amendment to these guidelines. By completing a User Agreement, users agree to comply with all terms and conditions of use below.

6 Terms and conditions of use

Users must comply with the following terms and conditions of use whenever they use ONYX:

1. Users must complete a User Agreement prior to using ONYX.
2. Usage accords with all relevant instruments or documents, including those outlined within these guidelines. Examples of this compliance includes users:
 - a. Not searching for any information unrelated to the course of their duties.
 - b. s37(2)(b)
 - c. Ensuring that all searches and use of resulting information obtained accords with the Australian Privacy Principles (APPs) and APS Code.
3. Users must report any of the following that occurs during searches:
 - a. Inadvertent accesses of information, including accessing accounts of their family, relatives, friends or associates.
 - b. Any content accessed that is explicit, criminal or highly sensitive in nature.
 - c. Posting of unlawful or prohibited content.
 - d. Communication initiated by account holders or other parties.
4. s37(2)(b), s47E(d)
5. Users must meet all relevant evidentiary, storage and record keeping requirements.
6. s47E(d)
7. s47E(d)

7 How to complete a User Agreement

- The process to complete a User Agreement is as follows - users:
- Create an email with the s47E(d)
- Include the following text s47E(d)
- Send the email to the Administrator at s47E(d) [@servicesaustralia.gov.au](mailto:s47E(d)@servicesaustralia.gov.au).
- CC their manager/s into the email.

8 Roles and responsibilities

8.1 Users

Users are responsible for the following:

- Before commencing to use ONYX, users must:
 - Ensure they have read these guidelines (including the terms and conditions of use in particular).
 - Complete a User Agreement.
 - Undertake sufficient training.
- When using ONYX, users must:
 - Comply with all terms and conditions of use.

8.2 Managers

Managers (Directors, Assistant Directors or Senior Analysts / Investigation Officers) are responsible for the following:

- Ensuring their staff have sufficient training before commencing to use ONYX.
- Managing and mitigating all relevant risks involving their staff. This includes risks of users being exposed to explicit, highly sensitive or unlawful content, which may require managers to ensure the ongoing wellbeing of these users as per the agency Work Health and Safety obligations.
- Monitoring the adherence of their staff to the terms and conditions of use.
- Helping other agency employees address any breaches of the terms and conditions of use or adverse audit findings involving their staff.

8.3 Administrator

- Assisting users and managers to help ensure Fivecast is being properly utilised. Examples are providing advice and support to users on request or updates from Fivecast on product changes, and escalating system issues to Fivecast for resolution.
- Assisting the agency to administer the use of Fivecast. Examples are helping ensure the contract is correctly managed, running monthly user reports to ensure the limited licences are being fully utilised, and assisting with any audits of usage.

9 Access, use and storage of information

9.1 Key principles

s47G, s47E(d)

s47G, s47E(d)

9.2 Before undertaking searches

s47G, s47E(d)

9.3 Undertaking searches

s47G, s47E(d)

9.4 Explicit, highly sensitive or unlawful content

s47E(d)

9.5 Documenting searches

s47G, s37(2)(b)

OFFICIAL: Sensitive

s47G, s37(2)(b)

9.6 Using findings

s47G

9.7 Storage of findings

s47G, s37(2)(b)

9.8 Disclosing findings

All disclosure of information collected via ONYX must accord with all relevant instruments or documents. These include, but are not limited to the following:

- The Australian Privacy Principles (APPs), in particular APP 11, which regulates how the agency regulates the disclosure of personal and sensitive information.
- All confidentiality and secrecy provisions within social security, families, health, child support and disability services law relevant to the use and release of personal or protected information.
- Agency information release policies.

OFFICIAL: Sensitive

10 Administration

10.1 Support and advice

The FDC Integrity Surge team administer ONYX usage within the agency, and are available to provide support to users and other agency employees regarding ONYX.

Staff are encouraged to contact the Administrator at the s47E(d) mailbox who can assist with all of the following:

- Providing advice and support on request.
- Additional advice or resources regarding the use of ONYX.
- General enquiries about the ONYX system.
- Escalating system issues to Fivecast for resolution.
- Advice and support regarding additional training or licences for business areas.

10.2 Auditing

Users may be subject to audits of their ONYX usage, which will be conducted in order to verify that their usage of ONYX is appropriate and meets all relevant terms and conditions of use.

servicesaustralia.gov.au



OFFICIAL

CIC Better Practice Guide

2.3 Capture & Storage of OSINT

Version: 1.0

s22 (out of scope)