




Department of the Premier and Cabinet  
Office of Digital Government

# Data Offshoring Governance

Guideline to support implementation of Western  
Australian Government Cyber Security Policy clause 1.5  
(Data Offshoring Governance)

*Includes WA Government Offshoring Position*





Produced and published by

**Department of the Premier and Cabinet  
Office of Digital Government**

Published **June 2025**

**Principal address:**

Dumas House  
2 Havelock Street  
West Perth WA 6005

**Postal address:**

Locked Bag 3001  
West Perth WA 6872

**Telephone:** (08) 6552 5000

**Fax:** (08) 6552 5001

**Email:** [Cyber.Policy@dpc.wa.gov.au](mailto:Cyber.Policy@dpc.wa.gov.au)

**Acknowledgement of Country**

The Government of Western Australia acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community. We pay our respects to all members of the Aboriginal communities and their cultures, and to Elders past, present and emerging.

**Approval**

Name / Title	Date
<b>Peter Bouhlas</b> <b>Chief Information Security Officer</b>	June 2025

**Contact Officers**

Name	Email	Phone
<b>Danijela Kambaskovic-Schwartz</b>	Danijela.Kambaskovic-Schwartz@dpc.wa.gov.au	+61 8 6552 6020
<b>Sandra Franz</b>	Sandra.Franz@dpc.wa.gov.au	+61 8 6551 3971



## Contents

<b>WA Government Cyber Security Policy clause .....</b>	<b>4</b>
1.5 Data Offshoring Governance.....	4
Responsibility for implementation .....	4
Purpose.....	4
<b>Data Offshoring Governance.....</b>	<b>5</b>
Offshoring Governance Process .....	5
Alternative arrangements - documenting Due Diligence and Risk Assessment Decisions .....	6
Reporting cyber security incidents to the Office of Digital Government .....	7
<b>WA Government Offshoring Position .....</b>	<b>8</b>
Scope.....	8
Background.....	8
Determining information confidentiality needs and information classification.....	9
The entity's information integrity and availability needs .....	10
Privacy .....	10
Personal Information .....	11
<b>Information subject to highest protection protocols (Tier 1 Risk).....</b>	<b>12</b>
Sensitive personal information .....	12
Digital identity.....	13
Other confidential information .....	13
Supporting Information.....	14
<b>Attachment 1: Office of Digital Government Information Security Risk Self- Assessment Table (A3) .....</b>	<b>15</b>
<b>Attachment 2: Office of Digital Government Information Security Risk Self- Assessment Table.....</b>	<b>16</b>



# WA Government Cyber Security Policy clause

Domain 1, **Govern**

## 1.5 Data Offshoring Governance

Each entity must define and understand its risks associated with data offshoring, with reference to:

- a. the [WA Government Data Offshoring Position and Guidance](#) (outlined below in this document)
- b. WA Government Cloud Policy
- c. WA Government Cyber Security Policy Implementation Guideline 3.4 (Information Secure Procurement) and the aligned Risk Assessment Template for procurement of cloud services
- d. Western Australian Information Classification Policy.

## Responsibility for implementation

Responsibility for implementing this clause lies with the Accountable Authority in collaboration with the Cyber Security Executive and the Chief Information Officer, as appropriate.

## Purpose

Due to the off-premises nature of cloud computing, it is common for WA Government information to be stored in locations and servers in different countries.<sup>1</sup> The act of storing WA Government information or transferring it to a location outside of the Commonwealth of Australia is known as “offshoring”.

The purpose of this document is to:

- Assist entities to implement the offshoring governance process for their entity.
- Articulate the WA Government Data Offshoring Position, intended to protect WA Government information and ensure its confidentiality, integrity and availability in the context of cloud computing.

---

<sup>1</sup> For the purposes of this document, the word the term ‘Information’ is used broadly and encompasses the terms, ‘information’, data’ and ‘records’ as used across the range of policy and legislation in Western Australia. This includes data and algorithms, digital and hard copy documents and correspondence, images, sound and video.





# Data Offshoring Governance

## Offshoring Governance Process


To establish robust information offshoring risk governance, entities should undertake the following process:

1. Review the [WA Government Offshoring Position](#).
2. Review all aspects of entity operations, procurement, use of service providers and their supply chain to identify entity data holdings which may be stored on the cloud and hosted outside Australia ("offshored"). These should be considered digital assets and inventoried.<sup>2</sup>
3. Identify all entity data holdings meeting [Tier 1 Risk](#) criteria.
4. Identify all entity data holdings meeting [Tier 2 Risk](#) criteria.
5. Perform and document the following tasks and processes:
  - a. Allocate corporate responsibility and deadlines for entity data discovery and classification.
  - b. Allocate corporate responsibility and deadlines for assessment of current cloud-related services and identify personal information covered by existing cloud service arrangements.
  - c. Where information is assessed as Tier 1 or Tier 2 risk to Government information and systems, plan to transition to Service Providers capable of hosting your information within Australia.
  - d. Ensure that any new Service Providers meet cyber security controls in accordance with the [WA Government Offshoring Position](#) and Office of Digital Government Information Secure Procurement Framework.<sup>3</sup>
  - e. If transition is temporarily impossible, allocate corporate responsibility and deadlines for implementing and documenting [alternative arrangements](#).
  - f. The [obligation to report any cyber security incidents](#) to the Office of Digital Government (DGov) within 6 hours of becoming aware of a cyber security incident.

---

<sup>2</sup> This asset identification work is relevant and will contribute to the entity meeting the WA Government Cyber Security Policy requirements 2.1 Cyber Security Context and 2.2 Cyber Security Risk Management.

<sup>3</sup> This will be published on wa.gov once approved. In the meantime, you can request an advanced copy from [cyber.policy@dpc.wa.gov.au](mailto:cyber.policy@dpc.wa.gov.au).



## Alternative arrangements - documenting Due Diligence and Risk Assessment Decisions

While the WA Government holds the position that it is safest for entity data classified as Tier 1 and Tier 2 Risk to be hosted in Australia, there may be circumstances, such as financial considerations or existing service contracts without break clauses, in which your entity may still decide to offshore information following a careful risk assessment.<sup>4</sup>



To appropriately record your risk assessment decisions within your offshoring governance processes, you should be able to present written records which demonstrate the following:

- The relevant manager with the [recorded allocated corporate responsibility for Data Offshoring Governance](#) is aware of and has listed all instances of your entity's data offshoring and the location of the relevant data centres, the associated Service Providers and dates contracts expire.
- You have assessed information security risks associated with high-risk locations.<sup>5</sup>
- You have a statement of assurance from your Service Provider advising you on how these risks are being managed.
- You have considered any legal and logistical implications for Tier 1 and Tier 2 risk information associated with your entity's information being hosted or accessed overseas.
  - for instance, if your data is hosted or accessed in Europe and involves personal information, your Service Provider holds GDPR certification
  - as another example, if your data is hosted or accessed in the United States, you, your Service Provider and your clients have access to cyber insurance.
- You can demonstrate that you have clarity and oversight over your Service Provider's cyber security posture.
  - that you have consulted the DGov Risk Assessment Template for procuring services offered by 3rd party Service Providers
  - that your Service Provider holds certification required for access to [Tier 1 / Tier 2 Risk](#) information

---

<sup>4</sup> For instance, if Sensitive: Personal information is being hosted within the European Union, it could be argued that the European privacy law, GDPR, is appropriately stringent and comparable to Australian privacy laws, which could suggest that clients' personal information will be protected similarly as in Australia.

<sup>5</sup> For additional information about country security, please see additional information in Office of Digital Government WA Government Cyber Security Policy Implementation Guidance 3.3 Enterprise Mobility. This will be published on [wa.gov](http://wa.gov) once approved. In the meantime, you can request an advanced copy from [cyber.policy@dpc.wa.gov.au](mailto:cyber.policy@dpc.wa.gov.au).

- 
- 
- you are satisfied that your Service Provider has an appropriately mature continuous monitoring and detection as well as incident handling procedures
    - your Service Provider agrees to let you know within 24 hours of any cyber security incidents that affect their systems.
  - You can demonstrate that you have considered the worst-case scenario.
    - you have documented your consideration of what may happen if your entity's information is breached while offshored, whether in transit or at rest
    - you have documented the support that your Service Provider will provide your entity in managing this incident and are satisfied that it is sufficient
    - you have documented the services that your Service Provider will make available to your entity's clients should their personal information be breached while offshored. You are satisfied that your entity's clients will have access to legal services, insurance and restitution of funds as appropriate
    - you have considered the financial or reputational damage that a breach of offshored data may cause your entity.



## Reporting cyber security incidents to the Office of Digital Government

Suspected or confirmed incidents, or any threat intelligence obtained by the entity should be reported to the Cyber Security Unit at DGov through the portal <https://irp.dpc.wa.gov.au> or, if not available, via email [cybersecurity@dpc.wa.gov.au](mailto:cybersecurity@dpc.wa.gov.au) or mobile at 1800 922 923 (1800 WA CYBER), available 24/7, within **6 hours**<sup>6</sup> of becoming aware of or suspecting the incident or receiving threat intelligence. The report must include:

- Type of incident/ threat intelligence.
- Indicators of compromise, if known.
- Tactics, Techniques and Procedures according to MITRE ATT&CK matrices.
- Impact to agency and whether a Business Continuity Plan has been activated.
- Whether a public announcement is required.

---

<sup>6</sup> The WA Government Cyber Security Policy requires entities to report cyber security incidents to DGov within 24 hours of detection. However, it is recommended to report suspected or confirmed cyber security incidents within a six-hour window to enhance response time.



Any information provided to DGov regarding incident management will be treated in the strictest confidence and only used for the purposes of incident management support.

## WA Government Offshoring Position

The Position requires that WA Government information that is considered to meet the criteria for [Tier 1 Risk to Government information and systems](#)<sup>7</sup> should be hosted in Australia.

If an entity offshores any of its information or has information integrity or availability needs that meet the requirements for [Tier 2 and Tier 3 Risk to information and systems](#), they should limit arrangements to countries of the Five Eyes alliance (Australia, New Zealand, United States of America, United Kingdom and Canada).

Privacy is an especially important concern in offshoring of data. Until the privacy provisions of the Privacy and Responsible Information Sharing legislation come into effect,<sup>8</sup> WA public sector entities must comply with the interim privacy position. This requires that agencies ensure their actions are consistent with the applicable Australian Privacy Principles set out in Schedule 1 of the *Privacy Act 1988* (Cth).

This Position applies in addition to the *State Records Act 2000* (WA). Any legal requirements relating to entity data are undiminished by the Position.

This Position is further clarified in the headings below.

### Scope

The Western Australian Government's Position on Offshoring applies to all entities included in the scope of the WA Government Cyber Security Policy.

This Position is supported by the [Office of Digital Government \(DGov\) Information Security Risk Self-Assessment Table](#) (Please refer to **Attachment 1**) and the Information Secure Procurement Framework.

### Background

Due to the off-premises nature of cloud computing, it is common for WA Government information to be stored in locations and servers in different countries.<sup>9</sup>


---

<sup>7</sup> Additional information security protections apply to Tier 1 Risk information. It must be encrypted at rest and in transit and Foreign Ownership risks must be considered when assessing potential service providers.

<sup>8</sup> The PRIS privacy provisions will come into effect when they are proclaimed.

<sup>9</sup> For the purposes of this document, the word the term 'Information' is used broadly and encompasses the terms, 'information', 'data' and 'records' as used across the range of policy and legislation in Western Australia. This includes data and algorithms, digital and hard copy documents, images, sound and video.





The act of storing WA Government information or transferring it to a location outside of the Commonwealth of Australia is known as “offshoring”.

In many cases, the specific location of the offshored data may not be clear under the cloud service agreement to the WA Government entity who is the information owner. Additionally, information may be stored in multiple locations.

Even where offshored information is held very securely, its mere existence in foreign jurisdictions means that it may be subject to the laws of that jurisdiction. This presents risks to WA Government data sovereignty, security, and privacy, especially when it comes to sensitive information, as well as prejudice legal access and insurance arrangements.<sup>10</sup>

## Determining information confidentiality needs and information classification

Information classification is a business process by which data or information is assessed and labelled according to the potential impact of its release. Information determined to be more sensitive typically requires different treatment and handling.

The Western Australian Information Classification Policy provides a common language for entities to identify risks and apply appropriate security controls to their information assets. It assists entities to determine their offshoring requirements for government information. The Policy requires that WA Government entities classify their information using the following categories.

- UNOFFICIAL (not relevant to data offshoring)
- OFFICIAL
- OFFICIAL Sensitive

Entities may also choose to apply the following sub classifications to OFFICIAL Sensitive information, where it requires special handling, or its use or disclosure is restricted under legislation:


- OFFICIAL Sensitive Cabinet
- OFFICIAL Sensitive Legal
- OFFICIAL Sensitive Personal
- OFFICIAL Sensitive Commercial

Based on the evolving threat landscape, the WA Information Classification Policy has recently been updated to include a new category:

- OFFICIAL Sensitive: [Digital Identity](#)

---

<sup>10</sup> Some nation states have legislation which requires their citizens (owners of digital service businesses) to disclose any foreign owned information stored in their systems on request.



This classification automatically applies where a document contains one or more categories of Personal information specified and discussed in the relevant section below.

## The entity's information integrity and availability needs

In addition to confidentiality of their information holdings, WA Government entities will have different needs when it comes to how available they need their information to be, as well as their tolerance for data corruption or loss and business disruption. These factors will greatly influence their offshoring requirements.

### Risk Self-Assessment

WA public sector entities should refer to the [Office of Digital Government Information Risk Self-Assessment Table](#) (**Attachment 1**) to assess the following risk factors, which will determine their approach to data offshoring:

- Does the information stored under the cloud service agreement include personal information and/or sensitive personal information?
- What is the classification (confidentiality or sensitivity) of other information that is stored under the cloud service agreement?
- What are the entity's needs when it comes to availability and integrity of their information?
- What is the entity's tolerance for business interruption?

## Privacy

Lack of public trust in government can hinder the uptake (and commensurate benefits) of better data-driven services. Open and transparent privacy management is a key component in building and maintaining that trust.

To protect the personal information of individuals and facilitate responsible sharing of government-held information, the WA Parliament has passed the *Privacy and Responsible Information Sharing Act 2024* (PRIS Act). Subject to decisions of government, it is anticipated that the privacy provisions will commence in 2026.

Until that time, the [interim privacy position](#) requires WA Government entities to ensure their actions are consistent with the [Australian Privacy Principles](#) (APPs).

The APPs are 13 principles set out in Schedule 1 of the *Privacy Act 1988* (Cth) that govern the rights, obligations and practices related to the collection, use and disclosure of personal information.

Where agencies are operating under statutes that contain specific provisions about the use or sharing of data, they should continue to comply with these.



## Personal Information

The interim privacy position applies to personal information, as defined in the PRIS Act.



This definition is broader than that under the *Privacy Act 1988* (Cth) and the *Freedom of Information Act 1992* (WA). Agencies should keep this in mind when following the interim privacy position.

The [PRIS Act](#) (section 4) defines **personal information** as follows:

- (a) means 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) includes 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.

The APPs include the following useful supplementary information regarding personal information:

- Personal information of one individual may also be personal information of another individual.
  - Examples include a marriage certificate that contains personal information of both parties to a marriage, and a vocational reference that includes personal information about both the author and the subject of the reference.
- The personal information 'about' an individual may be broader than the item of information that identifies them.
  - For example, a vocational reference or assessment may comment on a person's career, performance, attitudes and aptitude. Similarly, the views expressed by the author of the reference may also be personal information about the author.

- 
- 
- Personal information that has been de-identified will no longer be personal information.
    - Personal information is de-identified information if the identity of an individual is not apparent, and cannot reasonably be ascertained, from the information.
    - Under the PRIS Act, public entities must take reasonable steps to protect de-identified information from misuse and loss and from unauthorised reidentification, access, modification or disclosure.
  - What constitutes personal information will vary, depending on whether an individual can be identified or is reasonably identifiable in the particular circumstances.


## Information subject to highest protection protocols (Tier 1 Risk)

### Sensitive personal information

Not all information handled by Government entities is sensitive, or likely to give rise to significant privacy and security concerns. To protect the data without unduly restricting use of offshore services, the Western Australian Data Offshoring Position adopts the distinction between personal information and sensitive personal information according to the PRIS Act. Sensitive personal information is a subset of personal information that requires more stringent protection.

PRIS (section 4) defines **sensitive personal information** as 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.

## Digital identity

The changing threat landscape requires some personal information which can interact to form a “digital identity” to be given more stringent protection.

These types of personal information can be stolen, cross-referenced and used by malicious actors to steal an individual’s identity, usually for financial gain. Residential address is included in this list as it has relevance for an individual’s personal security.

If your data holdings contain **two or more** of the following types of personal information:

- **Name**
- **Date of Birth**
- **Government ID number**
- **Residential address**
- **Financial information.**

The updated Information Classification Policy requires that this data holding be classified OFFICIAL:Sensitive and [subject to the highest information security protocols](#).

## Other confidential information

- **Official Sensitive Commercial** is information that is required to be kept confidential because of a contractual or equitable obligation.
- **Official Sensitive Legal** is information that is required to be kept confidential because of legal professional privilege.
- **Official Sensitive Cabinet** is information that is required to be kept confidential because of the confidentiality of Cabinet deliberations.
- **Sensitive Aboriginal family history information** means information, including family history information, that —
  - (a) relates to Aboriginal people and their ancestors; and
  - (b) was collected in the period from 1898 until 1972 for the purposes of implementing laws, and government policies and practices, applying specifically to Aboriginal people.
- **Sensitive Aboriginal Traditional information** is information that, according to Aboriginal tradition, should not be disclosed to individuals who are not the knowledge holders of that information.





## Supporting Information

- [Australian Privacy Principles quick reference | OAIC](#)
- [Australian Signals Directorate: Cloud Security Guidance](#)
- [Information Management Framework for Western Australia](#)
- [Privacy Act 1988 \(Cth\)](#)
- [Public Cloud Cyber Risk Assessment](#)
- [State Records Act 2000 \(WA\) and State Records Commission Standards and Principles require that WA Government Entities “undertake appropriate risk assessments of data” before selecting storage or data centres of any kind.](#)
- [Submit a Freedom of Information \(FOI\) access application | Western Australian Government](#)
- [WALW - Privacy and Responsible Information Sharing Act 2024 - Home Page](#)
- [Western Australian Government Cyber Security Policy](#)
- [Western Australian Information Classification Policy](#)

## Attachment 1: Office of Digital Government Information Security Risk Self-Assessment Table (A3)

Risk Tier	Information Security Risk Self-Assessment Criteria					Information Security / Cyber Security - Next steps based on risk tiering			
	Confidentiality of Information		Availability of Information	Integrity of Information	Business Impact of Disruption	Cloud Services Offshoring (Data Sovereignty and Security)	Supplier Security	Personnel Security	Identity and Access Management
	Information Classification	Information Type							
<b>Tier 1</b>	<b>OFFICIAL SENSITIVE</b> (Additional criteria apply to Protected, Secret and Top-Secret Commonwealth information security classifications)	<b>OFFICIAL Sensitive Personal</b> ('sensitive personal information' as defined under the Privacy and Responsible Information Sharing Act 2024) <b>OFFICIAL Sensitive Cabinet</b> <b>OFFICIAL Sensitive Commercial</b> <b>OFFICIAL Sensitive Legal</b> <b>Digital Identity</b> (Two or more types of 'Personal information' as defined under the Privacy and Responsible Information Sharing Act 2024, as listed below): <ul style="list-style-type: none"> <li>Name</li> <li>Date of Birth</li> <li>Government ID number</li> <li>Residential address</li> <li>Financial information</li> </ul>	Service available at all times. (99.9% uptime) High Capacity or peak usage expected.	Reliably accurate. High level of accountability required (e.g. financial information).	High business impact. Impact to critical services. Impact to public safety	Must be hosted in Australia (preferably in two different locations). Security controls are in place for offshore backups or user access from offshore locations. Data Encryption at rest and in transit. Consider supplier Foreign Ownership risks.	Baseline information security considerations/ contract clause principles and Tier 1 information security considerations. Evidence of annual or biannual independent assessment of the information security risks associated with the service being procured (IRAP, ISO 27001, SOC2, FedRAMP). Foreign ownership/ board membership has been considered and is not a risk.	Individuals must have a police clearance. If in Australia, a regular police clearance. For individuals in the supply chain outside Australia, the requirement to guarantee the suitability of staff handling the information should be included in the contract with the main supplier.	Multi-factor Authentication
<b>Tier 2</b>	<b>OFFICIAL</b> (other types not included in Risk Tier 1)	Other types of ' <b>Personal information</b> ' (as defined in the Privacy and Responsible Information Sharing Act 2024) not specified in Risk Tier 1. Most government information and communication. Examples include content related to routine business operations and services and may include emails, memos and draft policies and guidelines on issues deemed to be non-sensitive.	Service available most of the time. Business continuity possible with short-term disruptions.	Reliably accurate.	Low/moderate business impact. Reduced efficiency and increased cost of operations.	Can be hosted outside Australia (requires a risk review if offshoring and assessment against Information Privacy Principle 9 when relevant provisions of the PRIS Act come into force). Limiting arrangements to countries of the Five Eyes alliance is strongly recommended (Australia, New Zealand, United States of America, United Kingdom and Canada).	Baseline information security considerations/ contract clause principles and Tier 2 information security considerations/contract clause principles. Supplier self-attestation against relevant information security requirements and regular reporting against compliance. Foreign ownership/ board membership has been considered and is not a risk.	Individuals must have a police clearance. If in Australia, a regular police clearance. For individuals in the supply chain outside Australia, the requirement to guarantee the suitability of staff handling the information should be included in the contract with the main supplier.	Multi-factor Authentication
<b>Tier 3</b>	<b>OFFICIAL (NOT CONFIDENTIAL)</b> Unofficial information is not relevant to procurement.	Public information. No high value information.	Can tolerate unavailability of service.	Lower integrity threshold.	Low/moderate business impact.	Can be hosted outside Australia (requires a risk review if offshoring). Limiting arrangements to countries of the Five Eyes alliance is strongly recommended.	Baseline information security considerations/ contract clause principles.	No specific requirements.	Multi-factor Authentication is recommended but not required.

# Attachment 2: Office of Digital Government Information Security Risk Self-Assessment Table

Risk Tier	Information Security Risk Self-Assessment Criteria					Information Security / Cyber Security - Next steps based on risk tiering			
	Confidentiality of Information		Availability of Information	Integrity of Information	Business Impact of Disruption	Cloud Services Offshoring (Data Sovereignty and Security)	Supplier Security	Personnel Security	Identity and Access Management
Tier 1	<b>OFFICIAL SENSITIVE</b>  (Additional criteria apply to Protected, Secret and Top-Secret Commonwealth information security classifications)	<b>OFFICIAL Sensitive Personal</b> ('sensitive personal information' as defined under the Privacy and Responsible Information Sharing Act 2024)  <b>OFFICIAL Sensitive Cabinet</b> <b>OFFICIAL Sensitive Commercial</b> <b>OFFICIAL Sensitive Legal</b>  <b>Digital Identity</b> (Two or more types of 'Personal information' as defined under the Privacy and Responsible Information Sharing Act 2024, as listed below): <ul style="list-style-type: none"> <li>Name</li> <li>Date of Birth</li> <li>Government ID number</li> <li>Residential address</li> <li>Financial information</li> </ul>	Service available at all times.  (99.9% uptime)  High Capacity or peak usage expected.	Reliably accurate.  High level of accountability required (e.g. financial information).	High business impact.  Impact to critical services.  Impact to public safety	Must be hosted in Australia (preferably in two different locations).  Security controls are in place for offshore backups or user access from offshore locations.  Data Encryption at rest and in transit.  Consider supplier Foreign Ownership risks.	Baseline information security considerations/ contract clause principles and Tier 1 information security considerations.  Evidence of annual or biannual independent assessment of the information security risks associated with the service being procured (IRAP, ISO 27001, SOC2, FedRAMP).  Foreign ownership/ board membership has been considered and is not a risk.	Individuals must have a police clearance.  If in Australia, a regular police clearance.  For individuals in the supply chain outside Australia, the requirement to guarantee the suitability of staff handling the information should be included in the contract with the main supplier.	Multi-factor Authentication
Tier 2	<b>OFFICIAL</b> (other types not included in Risk Tier 1)	Other types of 'Personal information' (as defined in the Privacy and Responsible Information Sharing Act 2024) not specified in Risk Tier 1.  Most government information and communication.  Examples include content related to routine business operations and services and may include emails, memos and draft policies and guidelines on issues deemed to be non-sensitive.	Service available most of the time.  Business continuity possible with short-term disruptions.	Reliably accurate.	Low/moderate business impact.  Reduced efficiency and increased cost of operations.	Can be hosted outside Australia (requires a risk review if offshoring and assessment against Information Privacy Principle 9 when relevant provisions of the PRIS Act come into force).  Limiting arrangements to countries of the Five Eyes alliance is strongly recommended (Australia, New Zealand, United States of America, United Kingdom and Canada).	Baseline information security considerations/ contract clause principles and Tier 2 information security considerations/contract clause principles.  Supplier self-attestation against relevant information security requirements and regular reporting against compliance.  Foreign ownership/ board membership has been considered and is not a risk.	Individuals must have a police clearance.  If in Australia, a regular police clearance.  For individuals in the supply chain outside Australia, the requirement to guarantee the suitability of staff handling the information should be included in the contract with the main supplier.	Multi-factor Authentication
Tier 3	<b>OFFICIAL (NOT CONFIDENTIAL)</b>  Unofficial information is not relevant to procurement.	Public information.  No high value information.	Can tolerate unavailability of service.	Lower integrity threshold.	Low/moderate business impact.	Can be hosted outside Australia (requires a risk review if offshoring).  Limiting arrangements to countries of the Five Eyes alliance is strongly recommended.	Baseline information security considerations/ contract clause principles.	No specific requirements.	Multi-factor Authentication is recommended but not required.