WA Government data offshoring position and guidance

WA Offshoring Position

The Western Australian Government's Position on Offshoring requires that WA Government information that is considered to meet the criteria for Tier 1 Risk to Government information and systems[1] 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[2], 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.

Purpose

The purpose of the WA Government Data Offshoring Position is to protect WA Government information and ensure its confidentiality, integrity, and availability.

Scope

The Western Australian Government's Position on Offshoring applies to:

- WA Public Sector as defined in the *Public Sector Management Act 1994* (WA)
- Schedule 1 entities as defined in the *Public Sector Management Act 1994* (WA), specifically:
    - The WA Police Force
    - Gold Corporation and Goldcorp Australia
    - Racing and Wagering Western Australia
    - Western Australian Land Authority
    - Department of the Staff of Parliament
    - WA Universities (Curtin University, Edith Cowan University, Murdoch University, The University of Notre Dame, The University of Western Australia)

[1] 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.

[2] The PRIS privacy provisions will come into effect when they're proclaimed.

    - All WA Government Trading Enterprises (GTEs), regardless of whether included in the Scope of the GTE Act 2023 and regardless of whether included in the scope of the *Security of Critical Infrastructure Act 2018* (Cth)
- Schedule 2 Senior Executive Service (SES) entities as defined in the *Public Sector Management Act 1994* (WA)
- Health Service and Health Service Providers (as defined in the *Health Services Act 2016* (WA)).
- Local Government and other entities not specified in the Scope are also encouraged to comply with the provisions of the Position.

This Position is supported by the Office of Digital Government's (DGov) Information Security Risk Self-Assessment Table (Please refer to **Attachment 1)** and 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.[3] 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.[4]

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

[3] For the purposes of this document, the wordthe term 'Information' is used broadly in this document 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.

[4] 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.

- 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.

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 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 ensuretheir 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 slightly wider than that under the Privacy Act 1988 (Cth) and *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 re-identification, 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 individually or together, cross-referenced and used by malicious actors to steal an individual's identity, usually for financial gain. This is why the following types of personal information (whether stored or shared in combination or not) should **also** be subject to the highest information security protocols even though they are not designated as sensitive personal information by the privacy legislation:

- Name
- Date of Birth
- Government ID number
- Residential address

- Financial information.

Please refer to the DGov Information Security Risk Assessment Table at Attachment 1.

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:

- WALW - Privacy and Responsible Information Sharing Act 2024 - Home Page
- *Privacy Act 1988* (Cth)
- Information Management Framework for Western Australia
- Submit a Freedom of Information (FOI) access application | Western Australian Government
- 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.
- Western Australian Government Cyber Security Policy
- Australian Signals Directorate: Cloud Security Guidance

Attachment 1: Office of Digital Government Information Security Risk Self-Assessment Table

Risk tiers	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							
Tier 1	**OFFICIAL SENSITIVE** **Protected** Commonwealth information security classification (Additional criteria apply to **Secret** and **Top-Secret** Commonwealth information security classifications) Certain Categories of **OFFICIAL**	**OFFICIAL Sensitive Personal** ('sensitive personal information' as defined under the Privacy and Responsible Information Sharing Act 2024) **OFFICIAL Sensitive Cabinet** **OFFICIAL Sensitive Commercial** **OFFICIAL Sensitive Legal** **Digital Identity** (Certain categories of 'personal information' as defined under the Privacy and Responsible Information Sharing Act 2024) - Name - Date of Birth - Government ID number - Residential address - Financial information	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). 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	**OFFICIAL** (other types not included in Risk Tier 1)	**Personal** 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	**OFFICIAL** (NOT CONFIDENTIAL) 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.