



Department of
the Premier and Cabinet

Western Australian Government Information Classification Policy

Business Impact Levels Tool

Version 6.0 | May 2026



Document Control

Title: Western Australian Government Information Classification Policy Business Impact Levels Tool

Produced and published by: Department of the Premier and Cabinet, Office of Digital Government, Western Australia

Contact:

Office of Digital Government
2 Havelock Street
West Perth WA 6005

Data.Sharing@dpc.wa.gov.au

Document version history

| Date | Author | Version | Revision Notes |
|-----------|------------------------------|---------|---|
| Dec 2018 | Office of Digital Government | 1 | Draft Business Impact Levels Tool |
| July 2020 | Office of Digital Government | 2 | Business Impact Levels Tool for ICWG review. |
| Nov 2020 | Office of Digital Government | 3 | Revision to refer to risks with serious consequences. |
| Jan 2021 | Office of Digital Government | 4 | Revision to align with PSPF. |
| Mar 2021 | Office of Digital Government | 5 | FINAL revised following ICWG comments. |
| May 2026 | Office of Digital Government | 6 | Updated to align with PRIS |




This document, the **Western Australian Government Information Classification Policy, Business Impact Levels Version 6** is licensed under a **Creative Commons Attribution 4.0 International Licence**. You are free to re-use the work under that licence, on the condition that you attribute the Government of Western Australia (Office of Digital Government) as author, indicate if changes were made, and comply with the other licence terms. The licence does not apply to any branding or images.

License URL: <https://creativecommons.org/licenses/by/4.0/legalcode>

Attribution: © Government of Western Australia ([Office of Digital Government](#)) 2020

Notice Identifying Other Material and/or Rights in this Publication:

The Creative Commons licence does not apply to the Government of Western Australia Coat of Arms. Permission to reuse the Coat of Arms can be obtained from the [Department of the Premier and Cabinet](#).





Business Impact Levels Tool

Purpose

This Business Impact Levels (BIL) Tool supports the Western Australian Government Information Classification Policy, a key policy that assists agencies in both enterprise risk management and information risk management.

Information management enables agencies to meet business, government and community needs and expectations. It involves ensuring the integrity of information and balancing the need to protect information with the need to ensure appropriate access.

Assessing impact or damage to individuals, organisations or the State interest

The BIL Tool provides a baseline standard for assessing the impact of information compromise, for all Western Australian public sector agencies. Application of the BIL Tool will assist agencies to clearly and consistently identify the sensitivity of their information and apply appropriate protective security measures.

The tool is provided for agencies to map common types of information within their work areas to the classifications established in the Policy.

Agencies are encouraged to identify examples of agency information that align with the sections of the table and provide them to staff to aid in decision-making.

All rows in the table should be considered, but not all rows will be applicable in all agency contexts. For example, the State Infrastructure row may never apply to certain agencies. It is acceptable to pass over rows that do not apply, as other rows will compensate for impact that is manifested in other ways.

If and when aggregated information is being considered, where multiple individual sources are combined, due consideration should be given for how that aggregation affects the impact. If an agency is considering aggregated information from multiple agencies, all agencies involved should be included in determining potential business impacts.

Agencies with specific operational scenarios that are not captured in the table may provide additional rows to guide their staff. Do NOT remove rows. For example, agencies with emergency services response requirements and associated impacts may add a row so long as it does not conflict with or duplicate existing guidance.

Classification levels

The majority of information created or processed by WA government agencies is OFFICIAL.

OFFICIAL is the default category for information related to routine agency business operations and services.

OFFICIAL Sensitive is information that, due to its sensitive nature, requires application of appropriate protection including access or disclosure restrictions.

OFFICIAL and OFFICIAL Sensitive are dissemination limiting markers (labels) and are not security classifications.

Cabinet information (as defined in the Cabinet handbook) must ALWAYS be classified OFFICIAL Sensitive.

Information that is Commonwealth SECURITY CLASSIFIED includes data covered under arrangements such as MOUs between jurisdictions for managing highly sensitive material.





Agencies handling Commonwealth SECURITY CLASSIFIED information are required to comply with the provisions of the relevant inter-jurisdictional agreement(s), including processes under the Commonwealth's Protective Security Policy Framework (PSPF).

Note that the PSPF clearly distinguishes between security classifications (which are applied to PROTECTED, SECRET and TOP SECRET information) and non-security classifications (for OFFICIAL and OFFICIAL Sensitive information).

In cases where an agency has WA specific information or datasets with Business Impact Levels above OFFICIAL Sensitive, for example protected witness information, agencies may use the PSPF processes to assess that information and may apply the labels and protections appropriate for SECURITY CLASSIFIED information.

PSPF procedures for the assessment, labelling and protection of SECURITY CLASSIFIED information are available at:


<https://www.protectivesecurity.gov.au/pspf-annual-release>



Business Impact Levels (BIL) Table

Agencies may only ADD new rows to provide examples. Existing rows may not be removed.

| | UNOFFICIAL | OFFICIAL | OFFICIAL Sensitive |
|--|--|---|---|
| Sample information types | UNOFFICIAL information refers to content that is not related to OFFICIAL work duties or functions. Examples include an invitation to a coffee catch-up with a friend, or discussions relating to out of work activities or schedules. | Information at this level refers to the majority of government information created, used or handled by agencies. This may include content relating to routine business operations, services and information in a draft format not otherwise captured by higher-level business impacts. If authorised for unlimited public release, information at this level may be released publicly or published. | Information at this level commonly includes sensitive material created, used or handled by agencies. This may include content that has limitations restricting its use, disclosure or dissemination. |
| Sub-impact category ↓ | | | |
| Potential impact on individuals from compromise¹ of the information | | | |
| Dignity or safety of an individual (or those associated with the individual) | N/A | Information compromise would result in no or insignificant damage to an individual (or those associated with the individual). Includes <i>personal information</i> as defined in the <i>Privacy and Responsible Information Sharing Act 2024 (WA)</i> (PRIS Act). This may include information or an opinion about an identifiable individual (e.g., members of the public, staff etc.) but does not include information defined as <i>sensitive personal information</i> under the PRIS Act. ² | Information compromise would result in limited damage to an individual or those associated with the individual. Limited damage is: <ul style="list-style-type: none"> • potential harm, e.g., injuries that are not serious or life threatening, or • discrimination, mistreatment, humiliation or undermining an individual's dignity or safety that is not life threatening. Includes information defined as <i>sensitive personal information</i> under the PRIS Act. ² |
| Potential impact on organisations from compromise of the information | | | |
| Entity operations, capability and/or service delivery | N/A | Information compromise would result in no or insignificant impact to routine business operations and services. | Information compromise would result in limited damage to entity operations. Limited damage is: <ul style="list-style-type: none"> • a degradation in organisational capability to an extent and duration that, while the entity can perform its primary functions, the effectiveness of the functions is noticeably reduced, or • minor loss of confidence in government. |
| Entity assets and finances e.g., operating budget | N/A | Information compromise would result in no or insignificant impact to the entity assets or annual operating budget. | Information compromise would result in limited damage to entity assets or annual operating budget. Limited damage is equivalent to \$10 million to \$100 million. |
| Legal compliance e.g., information compromise would cause non-compliance with legislation, commercial confidentiality or legal privilege | N/A | Information compromise would not result in legal and/or compliance issues. | Information compromise would result in: <ul style="list-style-type: none"> • issues of legal privilege for communications between legal practitioners and their clients • contract or agreement non-compliance • failure of statutory duty • breaches of information disclosure limitations under freedom of information, privacy or other relevant legislation. |
| Aggregated data ³ | N/A | Information compromise of an aggregation of routine business information would not result in damage to individuals, organisations or government. | Information compromise of a significant aggregated holding of information would result in limited damage to individuals, organisations or government. |
| Potential impact on government or the state or national interest from compromise of the information | | | |
| Policies and legislation | N/A | Information compromise would result in no or insignificant impact to routine business operations and services. | Information compromise would result in limited damage, impeding the development of operations or operation of policies. |
| State or national economy | N/A | Information compromise would result in no or insignificant impact to the state or national economies. | Information compromise would result in limited damage. Limited damage is: <ul style="list-style-type: none"> • undermining the financial viability of one or more individuals, minor Australian-based or owned organisations or companies • disadvantaging a major Australian organisation or company. |
| State infrastructure | N/A | Information compromise would result in no or insignificant impact to State infrastructure. | Information compromise would result in limited damage or disruption to State infrastructure. |
| International relations | N/A | Information compromise would result in no or insignificant impact to diplomatic activities. | Information compromise would result in minor or incidental damage or disruption to diplomatic relations. |



| | | | |
|--|-----|--|--|
| Crime prevention, defence or intelligence operations | N/A | Information compromise would result in no or insignificant impact to crime prevention, defence or intelligence operations. | Information compromise would result in limited damage to crime prevention, defence or intelligence operations including: <ul style="list-style-type: none">• impeding the detection, investigation, prosecution of, or facilitating the commission of low-level crime• affecting the non-operational effectiveness of Australian or allied defence forces without causing risk to life. |
|--|-----|--|--|



BIL table notes:

1. Information compromise includes, but is not limited to:

- loss
- misuse
- interference
- unauthorised access
- unauthorised modification
- unauthorised disclosure.

2. Section 4 of the PRIS Act provides definitions of personal information and sensitive personal information:

personal information –

- (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

sensitive personal information means personal information –

- (a) that relates to an individual's –
- (i) racial or ethnic origin
 - (ii) gender identity, in a case where the individual's gender identity does not correspond with their designated sex at birth
 - (iii) sexual orientation or practices
 - (iv) political opinions
 - (v) membership of a political association
 - (vi) religious beliefs or affiliations
 - (vii) philosophical beliefs
 - (viii) membership of a professional or trade association
 - (ix) membership of a trade union, or
 - (x) criminal record;
- (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.

Where compromise of personal information, especially sensitive personal information under the PRIS Act would lead to damage, serious damage or exceptionally grave damage to individuals, this information warrants classification.

3. A compilation of information may be assessed as requiring a higher security classification where the compilation is significantly more valuable than its individual components. This is because the collated information reveals new and more sensitive information or intelligence than would be apparent from the main source records and would cause greater damage than individual documents. When viewed separately, the components of the information compilation retain their individual classifications.

