Western Australian Information Classification Policy

Business Impact Levels Tool

Document Control

Title: Western Australian 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

dgov-adminstrator@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.

Business Impact Levels (BIL) Tool

Purpose

This Business Impact Levels (BIL) Tool supports the Western Australian Information Classification Policy (June 2020), a key policy that assists agencies in their management of information and also risk management.

The management of information enables agencies to meet business, government and community needs and expectations. It involves 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 high-level baseline standard for measuring the impact of information release, 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 (but 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 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/sites/default/files/2020-09/pspf--infosec--8--sensitive-classified-information.pdf.

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 **Sub-impact category** ⬇	UNOFFICIAL information refers to content that is not related to OFFICIAL work duties or functions. Examples can 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 and services and information in a draft format (not otherwise captured by higher-level business impacts). If authorised for unlimited public releases, information at this level may be released publically 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.
Potential impact on individuals from compromise [1] 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 personal information as defined in the *Privacy Act 1988* (Cth). This may include information (or an opinion) about an identifiable individual (eg members of the public, staff etc) but would not include information defined as "sensitive information" under the *Privacy Act 1988* (Cth).[2]	Information compromise would result in limited damage to an individual (or those associated with the individual). Limited damage is: • potential harm, for example 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.
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: • 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; and/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: • 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: • 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: • 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: a. loss b. misuse c. interference d. unauthorised access e. unauthorised modification f. unauthorised disclosure.

2. Section 6 of the *Privacy Act 1988* (Cth) provides definitions of 'personal information' and 'sensitive information':

'**personal information** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.'

'**sensitive information** means:

(a) information or an opinion about an individual's:

(i) racial or ethnic origin; or

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual orientation or practices; or

(ix) criminal record;

(that is also personal information); or

(b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information; or

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or

(e) biometric templates.'

Where compromise of personal information, especially sensitive information under the Privacy 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.