Western Australian Information Classification Policy

Supplementary Guide

Document Control

Title: Western Australian Information Classification Policy Supplementary Guide

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
Oct 2020	Office of Digital Government	1	First draft for ICWG comment.
Nov 2020	Office of Digital Government	2	Revised draft following ICWG comments
Jan 2021	Office of Digital Government	3	Revision for ICWG endorsement
Feb 2021	Office of Digital Government	4	Revised draft following ICWG comments
April 2021	Office of Digital Government	5	Draft for BATAC approval
May 2021	Office of Digital Government	6	Final following BATAC approval

Contents

Information Classification Policy: Supplementary Guide

This supplementary guide is designed to help agencies progressively implement the Western Australian Information Classification Policy through adopting a risk based approach to securing their information assets in a logical and staged manner.

Further support is provided in the documents and templates listed at the end of this Guide.

All agencies provide direction to their staff[1] on their responsibilities for maintaining proper standards for creation, management, maintenance and retention of records. Classification is a procedure that applies to prevent the unauthorised disclosure of official papers or documents supplied to or seen by staff in their official duties.

The Approach

The approach to implementation of the Policy requires an agency to:

- Systematically assess the risks to the agency's information assets;
- Design and implement controls to address the risks; and
- Adopt overarching management processes that are monitored, reviewed, and refined on an ongoing basis.

What is information classification

Information classification is a standard business process for the labelling and handling of all government information that applies to all the information created and/or handled by staff during an agency's operations.

> Information classification provides a uniform approach and common language to guide information sharing within and between agencies.

Note that classification does not determine access under the *Freedom of Information Act 1992* (WA).

The Policy defines a set of three essential classifications for data and information to establish this basic, common language across government: **UNOFFICIAL**, **OFFICIAL** and **OFFICIAL Sensitive**.

These classifications should be applied as a minimum classification for information created, used, managed and shared by WA government organisations.

> **OFFICIAL** is the default classification that applies to most agency information.

[1] Note that, for the purposes of the Policy, "staff" refers to all public sector employees, including people employed on full-time or part-time basis, or on casual, sessional, fixed term and other contracts.

Who is responsible for classifying information?

Just as public sector staff are accountable for the scrupulous use of government resources and records management, they are also accountable for ensuring the information they create and use (including from external sources) is managed appropriately. This includes classifying information so it can be appropriately discovered and shared.

When information is created, substantially altered or received, the originator or owner is responsible for conducting an information classification assessment and applying the appropriate labels.

When information is shared within or between agencies, the originating agency, or owner of the information, is responsible for determining the classification. Agencies (and agency partners) may not change the classification of information without the permission of the party they receive it from.

The process of classification

The process for Information Classification in your agency will be tailored to your specific processes. Business environments change over time as the nature of our work, and how we do that work, changes. Classifications and labelling should be kept as simple as possible to maintain flexibility in these changing environments.

Common elements for the process of classification are outlined below.

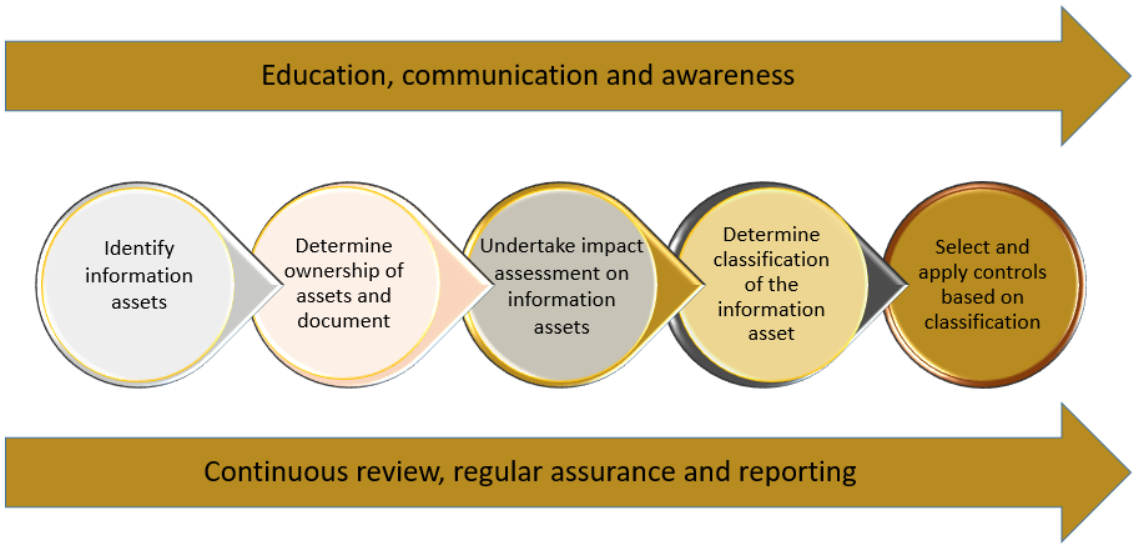


Figure 1 The information classification process

At its simplest, information classification follows a two-step process:

1. **Assess** the sensitivity of the information by undertaking a risk assessment of the impacts of the unauthorised disclosure of the information; and
2. **Label** it where appropriate, so that its sensitivity is clear to others.

1. Assessing the sensitivity of your information

The first step in Information Classification is to ask the question: “if this Information was released without authorisation, what would the impact be?”. This may be impact on your agency, on the government, on businesses, members of the public or a range of other stakeholders.

This process can be easily shaped to the typical business operations of your agency, so that a clear scale of potential impact is matched to the kinds of work your agency usually deals with and aligned with your agency's risk and information management frameworks.

The tool for assessing the sensitivity of information is a Business Impact Levels (BIL) table.

See the table provided at **Appendix A** for a high-level breakdown of Business Impact Levels.

The descriptions in the BIL table can easily be adapted to reflect the work undertaken by your agency, making the process more straightforward for your staff.

2. Selecting labels

The Western Australian Information Classification Policy establishes three classification labels: **UNOFFICIAL**, **OFFICIAL** and **OFFICIAL Sensitive**.

See the Information Classification assessment guide in **Appendix B** for advice on selecting labels for most of the information that WA agencies handle.

UNOFFICIAL
"Unofficial' information is unrelated to the official work of government.

Examples include personal emails or discussions related to out of work activities.

OFFICIAL
"Official" is the appropriate category for the vast majority of government information created, used or handled by agencies.

Examples include content related to routine business operations and services and may include emails, briefing notes, draft policies and guidelines on issues deemed to be non-sensitive.

Agencies must provide guidance, direction and training to their staff on the Public Sector Standards, Procedures and Regulations that apply to the creation, management, maintenance and retention of **OFFICIAL** information.

OFFICIAL Sensitive
"Official Sensitive" is the highest level of classification for information that is not covered under arrangements with other jurisdictions. Release of this information could result in damage to individuals, organisations or government.

Common examples in WA agencies include Human Resources documents, tender documents, and Cabinet documents.

Agencies must provide specific guidance, direction and training to their staff on the Public Sector Standards, Procedures and Regulations that apply to the creation, management, maintenance and retention of **OFFICIAL Sensitive** information.

Sublabels
Sublabels can be applied to **OFFICIAL Sensitive** information to denote where disclosure may be limited or prohibited by legislation, or where it may otherwise require special handling including limitations restricting its use, disclosure or dissemination.

It is important to consider whether this is necessary, as applying sub labels introduces complexities and overheads to managing the information.

Common examples in WA agencies include documents related to Cabinet records, legal advice, performance management of staff, and tender evaluations.

Agencies may choose to apply the following sublabels to **OFFICIAL Sensitive** information **only where absolutely necessary** to implement the Information Classification Policy:

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

Table 1: Approved sublabels for OFFICIAL Sensitive information

Sublabels	Description	Examples
Sensitive Cabinet	Information which is cabinet-in-confidence.	Cabinet documents, agendas and decision sheets.
Sensitive Personal	Information with personally identifiable and sensitive details.	Employee health files, banking information, HR records, performance management files.
Sensitive Commercial	Tender documents and information restricted by contractual conditions including non-disclosure agreements. Not to be used for general procurement contract correspondence–these should be classified **OFFICIAL**.	Tender documents and evaluation panel workbooks. Suppliers proprietary information, design or industrial secrets.
Sensitive Legal	Information subject to legal professional privilege.	Legal advice or communications.

In some rare instances agencies handle **OFFICIAL Sensitive** information where unauthorised disclosures may result in:

- Serious physical harm, life threatening injury, direct threat to life or loss of life;
- Impede the detection, investigation, prosecution of, or facilitate the commission of an offence with a penalty of imprisonment for two or more years; or
- Result in a major loss of confidence in the government.

Examples include documents related to witness protection or identification of a minor involved in Child Exploitation Material.

In the rare instances where WA agencies do have information or datasets with Business Impact levels above **OFFICIAL Sensitive**, they may use the Australian Government's Protective Security Policy Framework (PSPF) process to assess the information and apply the appropriate controls to label and manage the information.

COMMONWEALTH SECURITY CLASSIFIED INFORMATION

"**SECURITY CLASSIFIED**" information is information related to dealings with the Australian Government that has been denoted as being "**CLASSIFIED**". This information is covered under arrangements such as Memorandums of Understanding (MoUs).

The small number of agencies operating under these MoUs understand what they mean and are familiar with the requirements for using or handling **SECURITY CLASSIFIED** information.

Examples include national security information shared directly with the Australian Government.

Most agencies will never work with information in this category.

Information with **SECURITY CLASSIFIED** labels is subject to handling and physical security controls required by the PSPF.

> Applying PSPF requirements for information labelled as **OFFICIAL Sensitive** will severely limit the efficiency of day-to-day operations of your agency.

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).

3. Applying labels

By assessing the impact of unauthorised release of information up-front, your agency will have a clear guide for applying labels that is tailored to your business needs.

> Only apply labels to information as it is created or handled *as a minimum*.

Appendix C provides a flow chart of the general classification process.

Agencies may be proactive and apply labels to information in systems (e.g. as metadata).

Agencies are responsible for development of the standards or guides for Information Classification labelling and handling controls that apply in their agency.

This guidance must align with the agency's Code of Conduct, Record Management Plan, and information management and governance policies.

Agency guidance should include handling controls such as the examples provided in **Appendix D**. This guidance may define key roles such as those as referred to below and described further in Section 6.

Labels must be applied when:

- The information is created: the information owner must assess the consequences of damage from unauthorised release or misuse of the information. If adverse consequences could occur or if the agency is legally required to protect the information, the information must be labelled.
- Information is shared: the information owner must assess and label information prior to any use or sharing of information.
- Unlabelled information is received from external sources: the recipient must assess the information and label it.

Information custodians should provide appropriate classification and handling guidance to third parties requiring access to agency information.

Re-labelling of information from another agency is not necessary unless information has been added, edited or removed and the sensitivity has been changed. Re-labelling must be done in consultation with the information owner in the originating agency.

Archived material will only need to be assessed as it is retrieved.

The exchange of information often involves large numbers of datasets. In these instances, it may be appropriate to apply a label at the level of a set of datasets (or database etc).

Over classification
The default level of classification for government information is **OFFICIAL**. Higher levels of classification should only be applied when there is a clear and justifiable need - when the consequences of its unauthorised release warrants the expense of increased protection measures.

Over-classification can have a range of undesirable outcomes, including:

- Unnecessarily limiting public access to information;
- Unnecessary additional administrative arrangements and costs;
- Excess volumes of information for an agency to protect, at greater cost; and
- Devaluing higher classification labels so that they are ignored or avoided by employees or receiving agencies.

4. Design and implement controls based on the classifications

Once the classification has been determined, the appropriate controls for the management, handling, storage and retrieval of your information assets will need to be applied.

It is recommended that you seek advice on the most efficient way to apply controls from the supplier of your information management services. The Office of Digital Government (DGov) and State Records Office may also provide advice for certain commonly used systems.

These guidelines do not mandate specific security controls – your agency must select the controls best suited to your business and technology needs.

The controls must provide sufficient safeguards to adequately protect your information assets based on your assessment of the business impact of its unauthorised release.

5. Adopt overarching and ongoing management processes

Agencies are responsible for ensuring all their employees are scrupulous in the use of official records. This includes preventing the unauthorised disclosure[2] of official information, which may be a crime with penalties including up to three years' imprisonment.

In general, all government information must be:

- Classified to enable the information to be shared as openly as possible;
- Handled with due care and in accordance with authorised procedures, regulation and legislation; and
- Assessed against the impact that release of the information would cause your agency, the government or an individual.

Agencies may use their discretion to apply labelling for **UNOFFICIAL** and **OFFICIAL** information. Information assessed as **OFFICIAL Sensitive** or higher must be labelled.

> Agencies handling **OFFICIAL Sensitive** information **must** train staff in their standard operating procedures for labelling and handling that information.

[2] *Criminal Code of WA* Section 81 "Unauthorised disclosure" means disclosure of official information in circumstance where the person is under a duty not to make the disclosure.

Your agency's information classification and management is a living process that needs periodic and regular assessment as part of your arrangements for information governance.

For example, these reviews could be done after a project is completed or when a file is withdrawn from (or returned to) use. Information is declassified or reclassified to a lower classification when a reassessment of its Business Impact Level indicates it no longer meets the original Business Impact Level to which its classification applies.

6. Roles and Responsibilities

Your agency will need a documented policy or arrangement that defines how your organisation classifies and labels information, including the related roles and responsibilities for all staff.

These arrangements will be reported through your organisation's responsibilities under the *State Records Act 2000* i.e. your Records Management Plan and associated reporting.

Key roles referred to in these arrangements may include:

- Information owner:
  - any officer who receives, creates or manages information; and
  - is responsible for assessing the information and labelling it.
- Information asset owner:
  - any senior officer with accountability for an identifiable collection of information under legislation, regulation or policy;
  - is responsible for ensuring access to the information is monitored and complies with policy and legislation.
- Information asset custodian:
  - any agency officer with responsibilities to protect information assets including granting access, use and disclosure to the information;
  - is responsible for implementing and maintaining the information security requirements defined by the information asset owner.
- Information steward:
  - an agency officer with delegated authority for information assets as outlined in the relevant delegation schedule;
  - is responsible for ensuring that the management of information assets complies with legislation, policies, standards and MoUs.

Note that other role definitions may apply, for example within WA health system entities.

Agencies are responsible for applying the appropriate policies, procedures and or protocols for their information classification and management.

Agencies must advise all staff including contractors on the proper use of the agency's information classification, labelling and handling guidelines.

Further supporting documents

DGov has or will publish further supporting material in collaboration with the Information Classification Working Group. This material includes:

- Information Classification Assessment Flow Chart;
- Business Impact Levels (BIL) Tool;
- Templates and Guides for agencies to adapt:
  - Agency implementation roadmap template;
  - Agency policy template;

- Asset register template and guide;
- Education and awareness training guide.

Further guidance can be found in Public Sector Acts, Standards, and Policies including:

- Australian Standard AS 4120-1994 *Code of Tendering*;
- *Criminal Code Act Compilation Act 1913*;
- Department of Finance: *Procurement Practice Guide 2016*;
- Department of the Premier and Cabinet: *Cabinet Handbook 2020*;
- *Freedom of Information Act 1992*;
- Premier's Circular 2019/05 - *Cabinet Confidentiality;*
- Protective Security Policy Framework guidance documents: *https://www.protectivesecurity.gov.au/information/Pages/default.aspx*
- Public Sector Commissioner's Instruction No. 7: *Code of ethics*;
- *Public Sector Management Act 1994;*
- *State Records Act 2000;*
- State Records Commission Standards and Principles;
- State Supply Commission policies.

Appendix A: 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 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).	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	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.

Appendix B: Information classification assessment guide

Was the information created, sent or received as part of your work for the government?

Yes This is **OFFICIAL** information (baseline **Official**) and may need additional security protection including classification.

No

Consider

WOULD unauthorised disclosure result in low business impact, as the information consists of:

- Information collected from routine business operations and services and may include Personally Identifiable Information of an individual, business or entity?

Yes This information is **OFFICIAL -** the default category for most government information.

Consider

Is the information related to Cabinet business, or WOULD disclosure lead to (as a minimum):

- Potential harm, for example injuries that are not serious or life threatening;
- Compromise of **Sensitive** Personally Identifiable Information (as defined in the Commonwealth Privacy Act) resulting in discrimination, mistreatment, humiliation or undermining an individual's dignity or safety that is not life threatening;
- Loss of organisational capability causing a minor loss of confidence in government;
- Limited damage to government assets, infrastructure or operations and services, including closure or disruption;
- Impeding the detection, investigation, prosecution of, or facilitation of the commission of low level crime;
- Undermining the financial viability of individuals, organisations or companies; or
- Breach of legal privilege, tender processes, contracts or agreements, or result in a failure of statutory duty?

Yes This information requires the categorisation of **OFFICIAL Sensitive**.

Consider

Are any sub-labels appropriate? Agencies may choose to apply the following sublabels to OFFICIAL Sensitive information only where absolutely necessary.

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

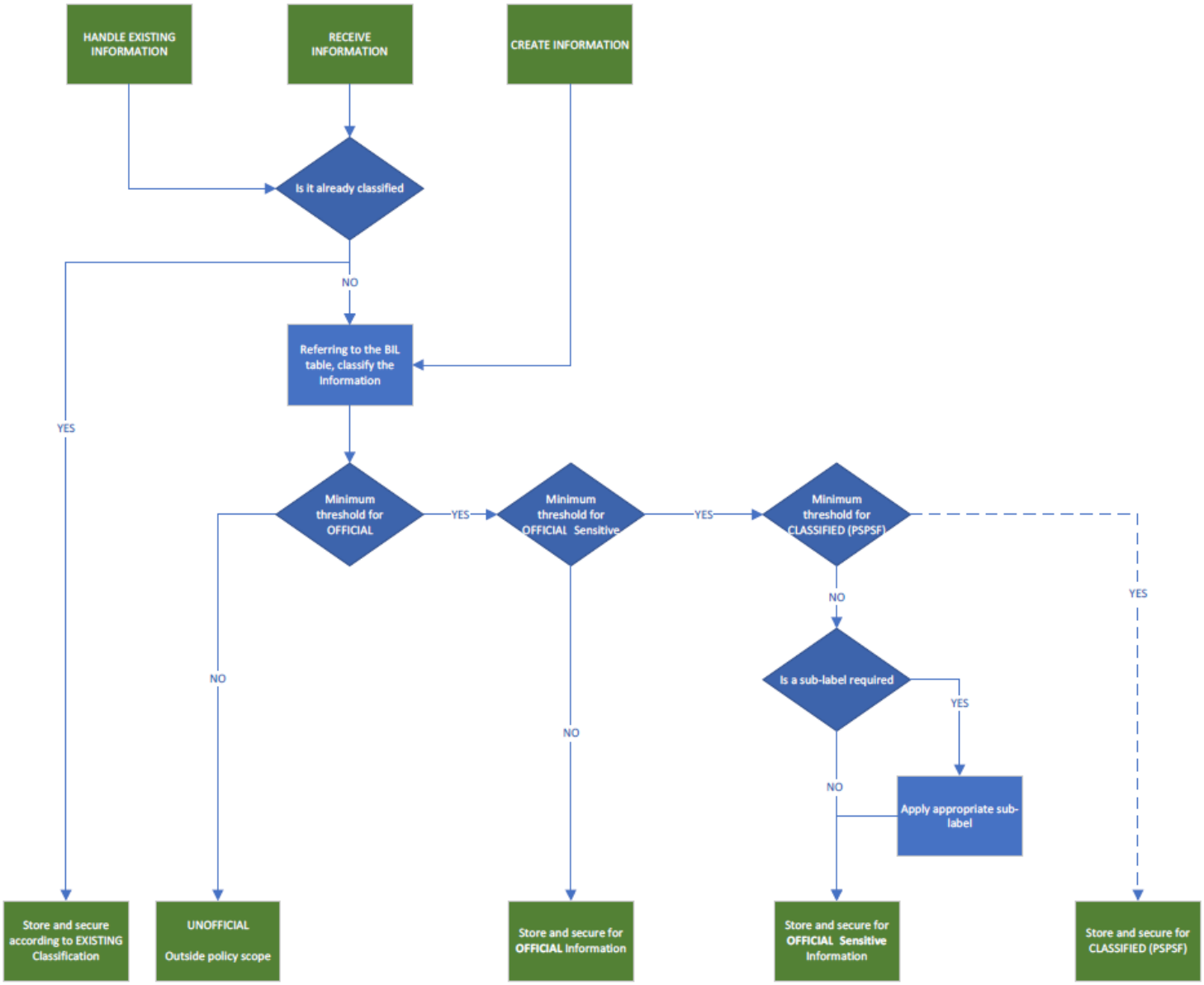
Consider

Is the information related to dealings with the Australian Government that they have denoted as being Classified (Protected, Secret or Top Secret)?

Yes Retain Australian Government security classification markers and note for further assessment.

No: This is **UNOFFICIAL** information.
Marking information as **UNOFFICIAL** is optional, but may be required by ICT system (e.g. email).

Appendix C: Information Classification process flow chart



Appendix D: Examples of Handling Controls

The following examples of handling controls for the different categories of information are provided for agencies to consider when developing Information Classification labelling and handling guides.

Refer also to the requirements of your agency's Code of Conduct and Records Management Plan.

For guidance on handling controls for Cabinet documents, tender evaluation documents and HR records that may be **OFFICIAL Sensitive** information, refer to public sector guidance such as the Cabinet Handbook, WA Government's Procurement Practice Guide, and the Public Sector Commissioner's Instructions.

UNOFFICIAL

Activity	Description
Not Applicable	• Controls not needed.

OFFICIAL

Activity	Description
Labelling	*Documents (Word, Excel, PDF):* • Clearly label **OFFICIAL**: bold text, large font, dark red in centre top of each page. • Clearly label prior to sharing documents. *Email*: • Clearly label: add **[OFFICIAL]** at the beginning of the subject field. • Turn on automated process where possible.
Storage	• Store, maintain and protect hard copy and electronic **OFFICIAL** information securely in accordance with your agency's Records Management Plan.
Transmission/Sharing	• Transfer, transmission and sharing of **OFFICIAL** information must follow the agency's authorised records management procedures.
Printing/Copying	• As required.
Retention and Disposal	• Dispose of hard copy and electronic **OFFICIAL** information in accordance with your agency's Records Management Plan, GDAs and/or Retention and Disposal Schedule.
Guidance & Training	• Provide guidance to all staff on the requirements of your agency's Information Classification Policy and Records Management Plan. • All staff must undergo record management awareness training to inform them of their record management roles and responsibilities.

OFFICIAL Sensitive

Activity	Description
Labelling	*Documents (Word, Excel, PDF):* • Clearly label **OFFICIAL Sensitive**: bold text, large font, dark red in centre top of each page. • Clearly label prior to sharing documents. • Apply additional labels where required: ○ **For example**: **OFFICIAL Sensitive Cabinet** documents may be stamped "Not to be copied" to reinforce confidentiality.

Appendix D: Examples of Handling Controls

	Email: • Clearly label: add **[OFFICIAL Sensitive]** at the beginning of the subject field. • Turn on automated process where possible. • Remind recipients that the contents are for their information only and are not to be forwarded on to unauthorised recipients. ○ **For example**: notify designated recipients of **OFFICIAL Sensitive Cabinet** documents in advance and remind them of Cabinet confidentiality requirements. *Metadata:* • Apply the Australian Government Recordkeeping Metadata Standard to protectively label information on any systems that store, process or communicate **OFFICIAL Sensitive** information.

Storage	• Allow access **ONLY** on to authorised officers.
	  ○ **For example**: access to **OFFICIAL Sensitive Cabinet** records is restricted and records should be retained in access controlled storage areas with access recorded in a register.
	  ○ **For example**: access to **OFFICIAL Sensitive Commercial** tender documents should be restricted to members of the tender evaluation panel.
	• Store, maintain and protect hard copy and electronic **OFFICIAL Sensitive** information securely in accordance with your agency's Records Management Plan and guidance such as the Cabinet Handbook and the WA Government's Procurement Practice Guide.
	  ○ **For example**: when you are not at your desk, store **OFFICIAL Sensitive Cabinet** documents in a locked cupboard or drawer.
	  ○ **For example**: **OFFICIAL Sensitive Commercial** tender documentation and information, including tender offers, must be stored securely to safeguard their confidentiality. The chair of the evaluation panel should collect evaluation notes at the end of the evaluation process.

Transmission/Sharing	• Transfer or share hard copy or electronic **OFFICIAL Sensitive** information **ONLY** in accordance with your agency's authorised records management procedures **AND** with the approval of the information owner.
	  ○ **For example**: **ONLY** transmit **OFFICIAL Sensitive Cabinet** documents over a secure file sharing system or approved records system as these systems have appropriate security controls and create an audit trail.
	  ○ **For example**: **OFFICIAL Sensitive Personal** information produced during a performance management process must be kept in trust and only divulged to those with a need to know.

Printing/Copying	• Apply secure printing methods using a PIN or pass card. • Printing or copying may be prohibited by the information owner. ○ **For example**: do not copy, scan or take a photo of **OFFICIAL Sensitive Cabinet** documents.

Appendix D: Examples of Handling Controls

Retention and Disposal	• Dispose of hard copy and electronic **OFFICIAL Sensitive** information in accordance with your agency's Records Management Plan, GDAs and/or Retention and Disposal Schedule. ○ **For example**: Archival **OFFICIAL Sensitive Cabinet** records **cannot** be disposed of, and eventually are housed in the State Archive Collection. ○ **For example: OFFICIAL Sensitive Commercial** tender documentation and information, including tender offers, should be retained for audit processes.
Guidance & Training	• Provide guidance to all staff on the requirements of your agency's Information Classification Policy and Records Management Plan. • Provide training to staff handling information or systems that store, process or communicate **OFFICIAL Sensitive** information such as procurement, HR or Cabinet records and make available appropriate guidance material to inform them of their responsibilities. ○ **For example**: staff involved in involved in handling **OFFICIAL Sensitive Commercial** documents during procurement processes should be trained in contract management and procurement practices to a suitable level aligned with the tender value and the agency's delegations schedule. ○ **For example**: staff involved in handling **OFFICIAL Sensitive Cabinet** documents should be made aware of the principles of Cabinet confidentiality and the processes required by the Cabinet Handbook.