Department of
the Premier and Cabinet

We're working for Western Australia.

Western Australian Government

Information Classification Policy

Document Control

Title: Western Australian Government Information Classification Policy

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	Discussion paper and draft Policy
June 2020	Office of Digital Government	2	Final Policy
September 2023	Office of Digital Government	3	Policy updated to remove references to out of date Policies and clarify guidance on the application of classifications and labels.

Purpose

The purpose of the Western Australian whole-of-government Information Classification Policy (the Policy) is to provide direction for Western Australian public sector agencies to label their information according to its sensitivity.

Scope

The Policy applies to all information generated, managed or shared by public sector agencies.

The Policy does not provide direction on digital security measures to protect information. This is provided through existing mechanisms and requirements, including other whole-of-government policies, agency-specific policies and Memorandums of Understanding (MOUs) between agencies and with other jurisdictions.

The Policy does not contradict, replace or otherwise affect agencies' legislative obligations, including those under the *State Records Act 2000*.

Objectives

The objectives of the Policy are to provide State Government with an information classification framework that enables agencies to:

- clearly and consistently identify the sensitivity of their information;
- apply appropriate protective security measures;
- communicate the sensitivity of information within the agency, with other agencies, and third-party organisations (where relevant);
- build a culture of trust for information sharing in the public sector, based on clear and widely understood labels;
- conduct an informed transition to new technology infrastructure based on sensitivity of information; and
- increase the security literacy and awareness of the public sector workforce.

Definition of Terms

Agencies – departments and Senior Executive Service (SES) organisations, as defined in the *Public Sector Management Act 1994*. This does not preclude non-SES organisations from participation, but this will not be mandatory.

Data - raw, unorganised and organised material such as characters, text, words, numbers, pictures, sound or video. It may be stored by both digital and non-digital means. Technically, data is a broader term than information, but "information classification" is preferred, as "information" is more commonly used in non-ICT contexts.

Information - organised, processed or structured data. For example, a graph which displays a bell-curve of test scores would be information, derived from the data of the individual scores. The term "information" can be taken to refer to both data and information for the purposes of the Policy.

Information classification – a business-level process whereby the sensitivity of a piece of information (or collection of information) is evaluated, and a classification label applied to it if appropriate, such that the sensitivity will be clear to those who access it subsequently.

The three classifications mandated under the Policy, align with the Australian Government's protective markings for non-security classified information in its Protective Security Policy Framework.

- UNOFFICIAL
- OFFICIAL
- OFFICIAL: Sensitive

Agencies handling COMMONWEALTH SECURITY CLASSIFIED information are required to comply with the provisions of the relevant inter-jurisdictional agreement(s) with the Australian Government.

The classifications represent the increasing sensitivity of the information and/or the type of information to which they are applied.

Sensitivity – the severity of negative consequences that are likely to result from the release of information. Sensitivity increases in line with the severity of the potential consequences.

Release – the making of information accessible to other individuals or organisations within and external to the agency responsible for the information, whether intentionally or unintentionally.

Label – a text addition to any given information, that represents its classification or sensitivity, such that it is clear to those who access the information.

The Risk Management Context

Information classification is primarily a risk management activity. Western Australian government agencies have risk management obligations, and generally have governance arrangements to enable them to meet these obligations.

Agencies can only make informed decisions regarding risk once they are aware of them. A risk-based decision making approach to information security and sharing of information requires clear oversight over the agency's information assets, which in turn requires the oversight of the peak corporate risk management body. Information classification is the responsibility of the entire business, not a delegated task for ICT teams. Integrating information classification into all areas of the business, with full corporate oversight, will enable agencies to ensure that information classification is appropriately planned, implemented and resourced within business needs and risk appetite.

Policy Requirements

The Policy requirements are as follows:

- The information classification process should be considered a part of core business and planning, not the delegated responsibility of ICT teams.
- Agencies are required to adopt the classifications defined above, in line with the guidance provided.
- When information is created, substantially altered or received, the originator or owner is responsible for conducting an information classification assessment and applying labels as appropriate.
- 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.

- Labels must be applied to information such that the label is clear, and wherever possible prior, to subsequent users accessing the information (e.g. a label in the header of an email; a clear marking at the top of a page).
- Agencies are required to ensure any party having access to the information is aware of and adheres to the Policy requirements.
- Agencies are not required to conduct a classification process on existing information or groups of information, until they are used (and then, in line with the agency's staged transition approach).
- Classifications applied to information should be re-assessed prior to any planned release, to account for the context of the release (e.g. information being shared in combination with other information which may combine to alter its significance).
- Security compliance:
  - For the protection of UNOFFICIAL, OFFICIAL, and OFFICIAL: Sensitive information, agencies are required to comply with the requirements of the relevant policies.
- Classification of information above OFFICIAL: Sensitive is outside the scope of this policy. Agencies should refer to the provisions of the relevant inter-jurisdictional agreement(s) regarding information at higher classification levels e.g., COMMONWEALTH SECURITY CLASSIFIED information.

Implementation

The policy should be implemented within five years from Cabinet approval. Agencies should assess their current capability and maturity, and where shortfalls are identified, develop a roadmap for achieving the requisite level of capability within the five years.

A five-year implementation timeframe will allow agencies to progressively implement the Policy and align their implementation activities with the renewal of ICT infrastructure.

Related Guidance

Additional supporting material to assist with implementation of the Policy is available from the Office of Digital Government website.

Agencies will need to ensure implementation of this Policy is consistent with, and operating within any applicable legislative, policy and strategic frameworks.

Policy Review

This policy is scheduled for review every five years or more frequently if required.