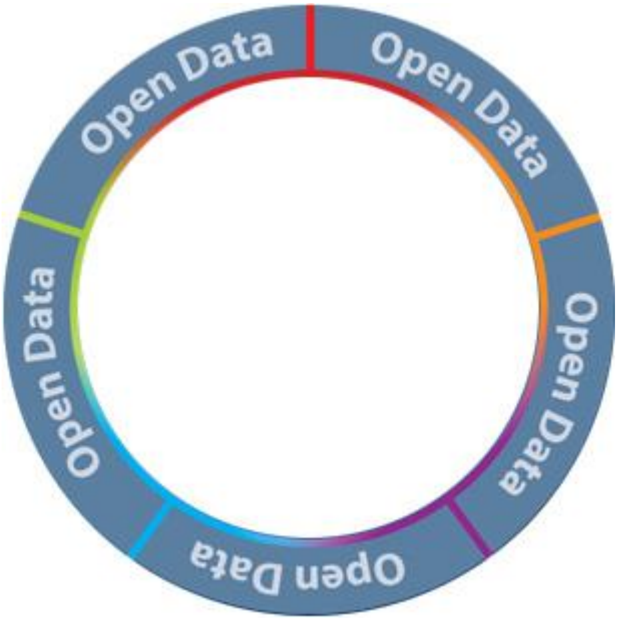
Government of South Australia

Office of the
Chief Information Officer



1.1

Office of the
Chief Information Officer

OPEN DATA GUIDE TO SECURITY CLASSIFICATION

Prepared by: Office of the Chief Information Officer
Version: 1.0
Date: November 2014

OPEN DATA GUIDE TO SECURITY CLASSIFICATION

Agencies should assess the data to determine if it could be released publicly, based on their Information Classification and marking procedures as required by the South Australian Government Information Security Management Framework (ISMF). Visit the Department of Premier and Cabinet website to the view the ISMF Policies and Standards. The Information Privacy Principals Instruction (IPPI) also guides information privacy in the Government of South Australia. View the IPPI (PDF 241Kb).

Data can only be marked as Public if the release of this information does not cause any damage to the state, the government, an agency, commercial entities or members of the public.

Only data that has been assessed and marked as Public can be released as open data. Data that has a Protective Marking or Dissemination Limiting Marker (refer ISMF), for example **Secret**, **For Official Use Only** or **Sensitive**, cannot be released as-is, however may be reclassified if appropriate declassification and/or risk mitigation activities are undertaken.

Responsibility and accountability

Chief Executives

Agency Chief Executives are accountable for all security matters within their agency. The Chief Executive must authorise the disclosure of all official information to the public.

Data Authority

The Data Authority is responsible for ensuring that classification/marking or re-classification/re-marking of the data is undertaken and that appropriate input is obtained from the data subject experts and information users.

Executive Peer Review

Executive Peer Review provides risk mitigation to ensure the public release of a dataset does not inadvertently put another part of the business security at risk or disclose information that could lead to identification of a person (mosaic effect).

Agencies are encouraged to conduct an Executive Peer Review of all dataset classifications and markings to confirm the dataset meets the requirements of Public, prior to release. Executive peer review is recommended if data has been manipulated to mitigate risks e.g. when personal information has been de-identified.

The recommended approach for an Executive Peer Review is to engage your Information Technology Security Adviser or Data Advocate to circulate open data candidates to all Executives within an agency for review and comment. A sample of the data should be provided and summary of how any data risks that have been mitigated e.g. de-identification techniques applied.

Agency Information Technology Security Adviser (ITSA)

Agencies should contact their Information Technology Security Adviser (ITSA) for further advice and guidance on agency specific information classification and marking procedures and guidelines. The ITSA should be consulted where appropriate in classification and marking decisions and can provide advice on threats and risks.

Security Classification and Markings Decisions

Data than can be made open must be assessed as meeting the requirements to be marked **Public.** Data marked as **Public** is authorised for unlimited public access and circulation such as agency publications, data download sites and websites.

Some data can be re-assessed and re-marked as **Public**. The data may require redactions, amendments or manipulation to ensure sensitive elements are removed so that there is no damage or potential damage to the government, business or members of the public. The Data Authority is responsible for re-classification and re-marking and should engage their ITSA to assist with these decisions and activities.

Security classification and marking decisions may identify data that contains some elements that needs to be protected or de-identified, please view the Privacy and Open Data Guideline for information on how to mitigate these risks.

Detailed instruction on how to protect sensitive elements of the data being considered for re-classification, is required to be documented in the open data process approval. An Executive Peer Review is recommended for data once these risk mitigation techniques are identified and applied in a sample of the modified dataset.

A Data Security Marking Decision Diagram based on the ISMF is provided (refer appendix A) to assist you to classify and apply appropriate markings. This following guidance is to be used in conjunction with this diagram to assist the user to understand each decision.

Security Classification and Markings Decision Guidance

1. Is the Data Security Classified Information?

National Security Classified information is any official information about, or is associated with Australia (including states and territories):

- security from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system or acts of foreign interference
- defence plans and operations
- international relations, significant political and economic relations with international organisations and foreign governments
- national or state interests, that relate to economic, scientific or technological matters vital to Australia's stability and integrity.

This type of information will be classified Confidential, Secret, or Top Secret as per *S19.7 ISMF. Only Government employees with a Security Clearance and need to know can access this information.*

Where a Data Authority considers a dataset to require a Security Protective Marking they should consult with their ITSA about the classification and appropriate controls to be applied.
Not eligible for open data

2. Would unauthorised disclosure of this data reveal South Australian Cabinet information?

Sensitive: SA Cabinet information includes:

- any document including but not limited to business lists, minutes, submissions, memoranda and matters without submission that is or has been:
  - submitted or proposed to be submitted to Cabinet
  - official records of Cabinet.
- any other information that would reveal:
  - the deliberations or decisions of Cabinet
  - matters submitted, or proposed to be submitted to Cabinet.

Where a Data Authority considers data to be Cabinet information they must apply a marking of ***Sensitive: SA Cabinet***
Contact Cabinet Office or State Records for more information on the release of this data. Certain Cabinet decisions or information may be releasable after a caveat date or media announcement (e.g. budget papers, major infrastructure initiatives etc.)

3. Would unauthorised disclosure of this reveal Sensitive Information?

Sensitive information includes:

- sensitive legal
- sensitive commercial
- sensitive medical - practitioner-patient privilege

a. Sensitive: Legal

Datasets containing information subject to court orders, legal proceedings or legal professional privilege, must not be made available under the Policy unless appropriate approvals are obtained.

Legal Professional Privilege protects all communications between a professional legal adviser (a solicitor, barrister, or attorney) and his or her clients from being disclosed without the permission of the client.

Where a Data Authority considers data to be subject to legal proceedings they must apply a marking of ***Sensitive: Legal***
Not eligible for open data

b. Sensitive: Commercial

Commercially sensitive data is any information, whose compromise could affect the competitive process and provide the opportunity for unfair advantage including:

- information concerning the trade secrets of any person
- information (other than trade secrets) that has a commercial value to any person
- any other information concerning the business, professional, commercial or financial affairs of any person
- likely to harm the business’s commercial advantage in the marketplace.

Sensitive data should not preclude the release of other valuable data from being released from a dataset. It may be possible to remove data that is commercially sensitive from a dataset and this new dataset could be assessed for open data purposes. Controls should be put in place to ensure sensitive information is removed. Refer to Section 27 Freedom of Information Act (SA)—Documents affecting business affairs for more information.

If classification and marking decisions identify data that contains some elements that needs to be protected or de-identified please view the Privacy and Open Data Guideline for information on how to mitigate privacy risks.

Note: you are assessing the content of the data and not any contractual arrangement for the provision of data when determining the sensitive nature of the data.

Where a Data Authority considers data to be commercially sensitive they must apply a marking of ***Sensitive: Commercial***
Not eligible for open data

Document whether data elements can be protected or de-identified as per the Privacy and Open Data Guideline**.**
Once protection techniques are applied, the Data Authority can re-asses and re-mark the data as Public.
ITSA advice and an Executive Peer Review of this data may be required.

c. Sensitive: Medical

Health professionals and services are under a strict ethical and legal duty to keep patient information confidential. A health professional may only provide information to a person other than the patient for reasons of significant public interest or when required by *legislation*.

Healthcare enactments or other medical industry legislation may also apply.

Where a Data Authority considers data to be subject to *medical practitioner patient privilege* they must apply a marking on the data as ***Sensitive: Medical***
Not eligible for open data

4. Would unauthorised disclosure of this data reveal sensitive data protected under legislative or secrecy provisions?

Agencies operate under various legislative provisions or secrecy provisions that specify conditions for restricting access or release of data e.g. *Public Sector Act* 2009 or the *Taxation Administration Act* 1996. The Declaration of Open Data does not supersede existing legislation. Agencies may be subject to other legislation particular to their business that specifies conditions for restricted access and/or release of their datasets. Data Authorities are encouraged to seek advice from their in-house legal advisors in relation to specific legislation they administer and any restrictions that may preclude the release of data.

Consider any third party rights concerning the use of information collected that was identified in the Open data process - identification stage.

It may be possible to remove the restricted data from the dataset and this new dataset could be assessed for open data purposes. Transformation and data amendments controls should be put in place to ensure restricted data is not released.

If security classifications or marking decisions identify data that contains some elements that needs to be protected or de-identified please view the Privacy and Open Data Guideline for information on how to mitigate privacy risks.

Where a Data Authority considers data to reveal sensitive data protected under legislative or secrecy provisions they must apply a marking on the data as ***Sensitive citing the provision*** (e.g. Pursuant to section 15 of the xx Act 1915).
Not eligible for open data

Document whether data elements can be protected or de-identified as per the Privacy and Open Data Guideline**.**
Once protection techniques are applied, the Data Authority can re-asses and re-mark the data as Public.
ITSA advice and an Executive Peer Review of this data may be required.

5. Would unauthorised disclosure of this data reveal personal information as described in the Privacy and Open Data Guideline?

Information privacy in the Government of South Australian is guided by the Information Privacy Principals Instruction (IPPI) issued as Premier and Cabinet Circular No 12 to regulate the way personal information can be collected, used, stored, and disclosed by State Government agencies.

The primary risk to privacy in the release of government data is the identification of individuals or data that can be made into personally identifiable information through easily linking with other information.

Privacy and Open Data Guideline

The Privacy Committee of South Australia has released the Privacy and Open Data Guideline to assist the government to maintain high standards of privacy when making its data open by default. Personal information of private citizens will not be released through open data. View the Privacy and Open Data Guideline.

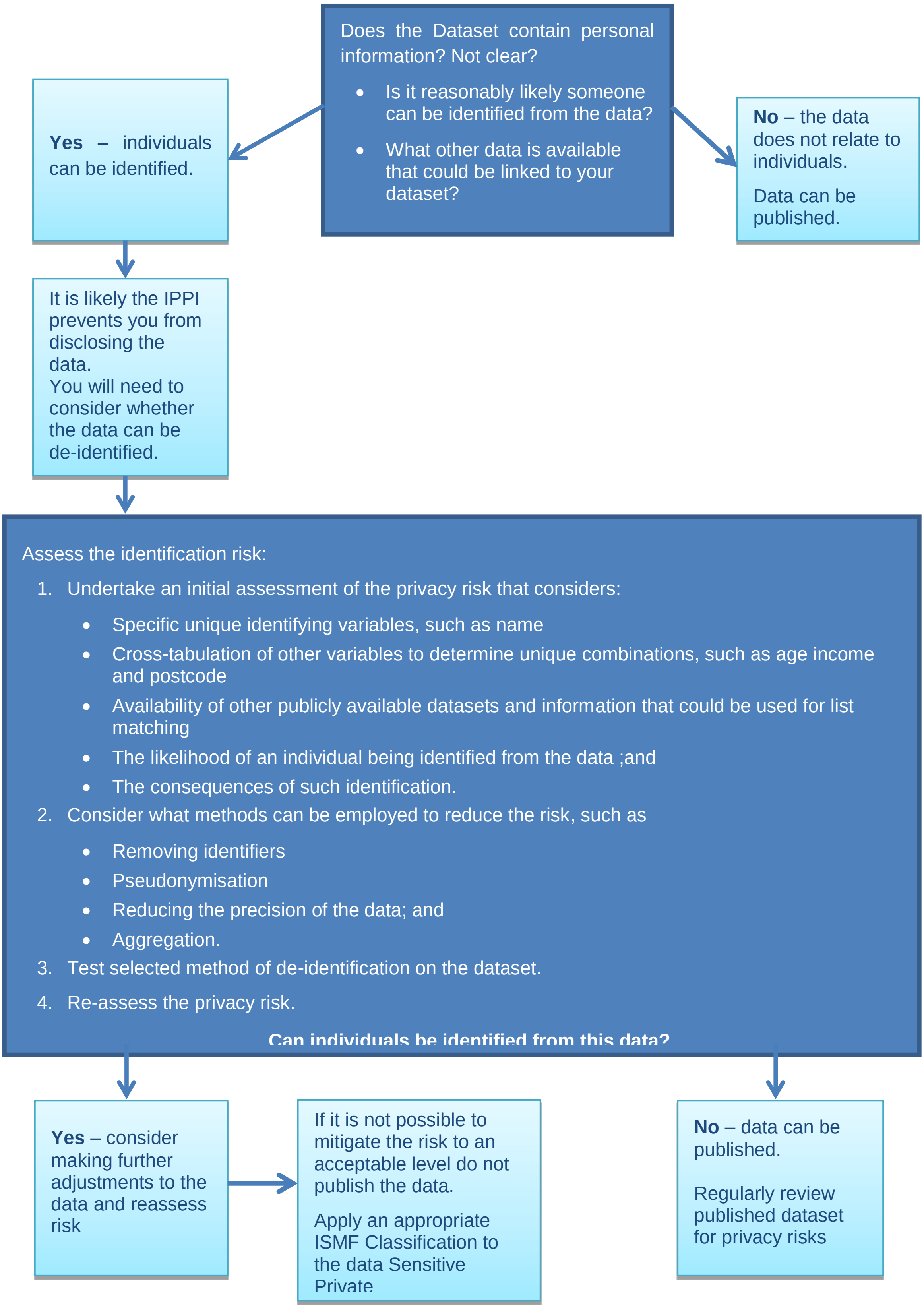
Privacy Risk Assessment

The Data Authority is responsible for ensuring that a Privacy Risk Assessment has been conducted to identify privacy risks, consider de-identification and detail transformation requirements.

Executive Peer Review is recommended if data has had protection techniques applied to mitigate risks e.g. when personal information has been de-identified.

The following *Privacy Risk Assessment Process* will assist agencies to identify risks.

PRIVACY RISK ASSESSMENT PROCESS



Does the Dataset contain personal information? Not clear?

- Is it reasonably likely someone can be identified from the data?
- What other data is available that could be linked to your dataset?

Yes – individuals can be identified.

No – the data does not relate to individuals.

Data can be published.

It is likely the IPPI prevents you from disclosing the data.
You will need to consider whether the data can be de-identified.

Assess the identification risk:

1. Undertake an initial assessment of the privacy risk that considers:
   - Specific unique identifying variables, such as name
   - Cross-tabulation of other variables to determine unique combinations, such as age income and postcode
   - Availability of other publicly available datasets and information that could be used for list matching
   - The likelihood of an individual being identified from the data ;and
   - The consequences of such identification.
2. Consider what methods can be employed to reduce the risk, such as
   - Removing identifiers
   - Pseudonymisation
   - Reducing the precision of the data; and
   - Aggregation.
3. Test selected method of de-identification on the dataset.
4. Re-assess the privacy risk.

Can individuals be identified from this data?

Yes – consider making further adjustments to the data and reassess risk

If it is not possible to mitigate the risk to an acceptable level do not publish the data.

Apply an appropriate ISMF Classification to the data Sensitive Private

No – data can be published.

Regularly review published dataset for privacy risks

For more information about a **Privacy Risk Assessment** refer to the Privacy and Open Data Guideline

Conduct a **Privacy Risk Assessment** as per the Privacy and Open Data Guideline.
Where a Data Authority considers data to include personally identifiable information they must apply a marking on the data of ***Sensitive: Personal***

Document whether data elements can be protected or de-identified as per the Privacy and Open Data Guideline**.**
Once protection techniques are applied, the Data Authority can re-asses and re-mark the data as Public.
ITSA advice and an Executive Peer Review of this data may be required.

6. Is the information ready for public distribution or posting (Public)

The Open Data Declaration requires Public data to be open by default and therefore "Official Use" of data should only be applied to information that is not for use or of benefit to the public at large.

Data may require caveats for confidentiality before release (e.g. Budget papers). In this case, the point at which the information will be entered in the public domain should also be specified. When this information ceases to need confidential treatment, agencies must continue to consider reclassification to public. It is recommended to continue the open data process for this type of data to plan the approach and seek approval for future release.

Some data may pose a moderate security threat. A moderate security threat is when government data, whose compromise could affect:

- the government's capacity to make decisions or operate
- the public's confidence in government
- the stability of the market place
- law enforcement operations, whose compromise could hamper or inhibit crime prevention strategies or particular investigations or adversely affect personal safety.

The government holds considerable information that was created for an official purpose, however on further review could be valuable information to stimulate innovation, the economy, and open access of information to the community. Data marked *For Official Use Only* can be reclassified as Public. Agencies should consider what steps are required to make data fit for use.

Data that could pose a moderate security threat must be classified as ***For Official Use Only.***
Data that is classified as ***For Official Use Only*** may define a caveat date for publication or steps that would be required to make data fit for public use. For this data it is recommended to continue with the open data process to determine if it should be released as open data at a later stage.
Once protection techniques are applied, the Data Authority can re-asses and re-mark the data as Public.
ITSA advice and an Executive Peer Review of this data may be required.

Marking data as Public

This data is authorised for unlimited public access and circulation, such as agency publications and web sites and as open data. Marking data as Public indicates that the data is a candidate to consider for open data and the open data process should be progressed.

Where a Data Authority considers data can be released for unlimited public access they must apply marking of ***Public***.
Eligible for Open Data