DATA CLASSIFICATION AND MARKING DECISION DIAGRAM

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

With the exception of the Government of South Australia brand, logo’s and any images, this work is licensed under a Creative Commons Attribution (BY) 4.0 Licence. To attribute this material, cite the Office of the Chief Information Officer, Government of South Australia, Data classification and Marking Decision Diagram, 2014.
Is the data associated with National security or State economic, scientific, critical infrastructure or technology interests vital to stability and integrity? (Only Government Sector Employees with Security Clearance should have access to this data.)

No

This data is considered Security Classified. Contact the Office of the CIO

Yes

Would unauthorised disclosure of this data reveal SA Cabinet information?
Generally this data is classified as Sensitive: SA Cabinet at the time it is created and access restricted.

No

This data requires the DLM Sensitive: SA Cabinet. Contact Cabinet Office as some information may be classified as Sensitive: SA Cabinet but may be approved for release after a particular date/event.

Yes

Would unauthorised disclosure of this data reveal data that may be subject to legal professional privilege, reveal sensitive commercial data that may give unfair advantage to a company, reveal commercially confidential information or reveal data that may be subject to medical practitioner-patient privilege?

No

This data requires a DLM Sensitive marking of either: Sensitive: Legal Sensitive: Commercial Sensitive: Medical

Yes

Would unauthorised disclosure reveal data protected under Legislative or Secrecy provisions?
Check the legislation or secrecy provisions that the data collection is authorised

No

Can protected data be removed or an aggregated version of data be created that will still provide value from the data

No

This data requires the DLM Sensitive citing the provision. (e.g. Pursuant to section 15 of the xx Act 1915)

Yes

This data must be considered ‘For Official Use Only’ and documentation of the amendments required. The data can be re-classified as Public once the amendments have occurred. ITSA advice is recommended

Can privacy/risk be mitigated through amendment?

This data requires the DLM ‘For Official Use Only’ Document any actions required for the data to be made public or caveats applied. A reclassification of this data as Public should be considered if appropriate once ready for distribution.

No

This data requires the DLM ‘Sensitive: Personal’

Yes

This data should be marked PUBLIC

No

This data is sensitive and should be Marked as ‘Sensitive:Personal’ and documentation of the de-identification required. The data could be re-classified as Public once the de-identification has occurred if the data is still of value.

Yes

Conduct a Privacy Risk Assessment. See Privacy & Open Data Guideline

Is this information ready for public distribution or posting?
Consider if the data would pose a moderate security threat. Data classified as Public is authorised for unlimited public access or circulation

No

Can privacy/risk be mitigated through amendment?

Yes

For more information refer to the Open Data Guide to Security Classification

For assistance and explanation of each decision point contact your Agency ITSA.