

Implementing the Information Security Classification Framework in Recordkeeping Systems

This public records brief outlines issues to consider when implementing the Queensland Government Information Security Classification Framework in Recordkeeping Systems. The Brief was developed in consultation with the Queensland Government Chief Information Office.

What is the Information Security Classification Framework?

The Queensland Government Information Security Classification Framework (QGISCF) sets out guidelines for the appropriate security classification of information assets in agencies. It is issued under *Information Standard 18: Information Security*. Principle 2 of IS18 states that agencies must ensure that:

- the classification of all information is in accordance with Queensland Government Information Security Classification Framework - Section 2; and
- the control of all security classified information (including handling, storage, transmission, transportation and disposal) is in accordance with Queensland Government Information Security Classification Framework - Section 5.

Does my agency need to implement the QGISCF?

Only those agencies subject to IS18 need to implement the QGISCF. As IS18 is not issued under the *Public Records Act 2002*, it does not apply to all public authorities. It only applies to Departments and Statutory Bodies under the *Financial Administration and Audit Act 1977*.

Public authorities, such as Local Governments, that are not required to implement IS18 may choose to adopt the QGISCF, if it is useful for their information management needs. For example, adherence to the requirements of IS18 also supports compliance with Principle 5: Recordkeeping systems must be reliable and secure, of *Information Standard 40: Recordkeeping*.

QGISCF in recordkeeping systems

Most electronic document and records management systems (eDRMS) and records management software contain provisions to identify the security classification of a record. The QGISCF provides a standardised set of information security classifications and treatments to ensure consistency across government agencies.

An information security classification may be applied at the file level or document level. When dealing with physical records, the security classification is normally applied to a file and all documents in the file 'inherit' this classification. In an eDRMS, it is also possible to apply information security classification at the document level. In this situation, either the file will be managed in accordance with the highest classification on it, or access will be restricted or permitted on a document by document basis.

Access control in an eDRMS

Control of access to sensitive records in an eDRMS is often applied through groups linked to user profiles: a user in the system is a member of a particular group (for example 'HR staff') and certain records (for example, personnel files) may only be accessible to users in a relevant group.

Information security classification does not replace the need for this type of group-based security. A key principle in the QGISCF is 'need to know' – for example, a person cannot access all information at a particular classification level, as they also must have a need to access the information, to do their work or for the efficient conduct of business. Group-based access complements information security classification by enforcing this 'need to know' access. As a result, an eDRMS will contain both information security classifications and group-based access controls.

QGISCF and physical records

The QGISCF also applies to physical records. Section 5 of the framework details the types of physical controls that must be applied to records of different information security classifications, including markings on file covers, appropriate storage and handling protocols, and methods of destruction. For example, the IN-CONFIDENCE, PROTECTED and HIGHLY PROTECTED classifications, require storing physical copies in lockable cabinets of varying specifications.

Responsibility for setting the classification in a recordkeeping system

Section 2.6 of the QGISCF sets out roles and responsibilities for information security classification. In practice, recommended or default information security classifications may exist for certain types or 'domains' of information – for example, all HR paperwork is STAFF-IN-CONFIDENCE or all procurement is COMMERCIAL-IN-CONFIDENCE. Other areas may routinely produce information with a PUBLIC classification. The record classes identified in your agency's Retention and Disposal Schedule may provide a framework for setting security classifications.

Responsibility for applying the correct information security classification in a recordkeeping system depends on the recordkeeping procedures of each public authority. For example:

- The end user may be required to select an information security classification when registering a document in an eDRMS, or
- Records management staff may apply the information security classification when creating a file.

Information security classification prompts and reminders should be built into relevant work procedures, and if end users are responsible for applying the security classification, quality assurance procedures should be in place to ensure consistent and appropriate application.

Relationship between QGISCF and recordkeeping metadata

The *Queensland Recordkeeping Metadata Standard and Guideline* complements IS18 and QGISCF by identifying Security Classification as required metadata. In accordance with the QGISCF, the Recordkeeping Metadata Standard also allows for 'Determination Date' or the date that the classification was made, and a 'Review due date' to trigger a review of the security classification.

As outlined in section 3.4.1 of the QGISCF, it is important to limit the duration of security classification, as sensitivity often decreases over time.

The QGISCF is available within the IS18 toolbox at <http://www.qgcio.qld.gov.au/qgcio/architectureandstandards/informationstandards/toolbox/Pages/Information%20Security.aspx>. For more advice on IS18 or the QGISCF and its application, please contact the QGCIO on (07) 3405 6222 or qgcio@publicworks.qld.gov.au.

The Queensland Recordkeeping Metadata Standard and Guideline is available on Queensland State Archives' website at <http://www.archives.qld.gov.au/downloads/QRKMS.pdf>.

For more detailed guidance on the management of public records visit the Queensland State Archives' website at <http://www.archives.qld.gov.au>, or contact us on:

Telephone: (07) 3131 7777

Email: info@archives.qld.gov.au