



Queensland Government Information Security Classification Framework

Version 1.0.0

November 2006

Queensland Government Chief Information Office

Document Details

Document Name	Queensland Government Information Security Classification Framework			
Version Number	Endorsed v 1.0.0			
Publication Date	3 November 2006			
Security Classification	PUBLIC Date of review of security classification January 2009			
Authority	Endorsed by the CIO Executive Council, 3 November 2006			
Author	Queensland Government Chief Information Office Jeff Tendero, Vanessa Freke, Allan Klason, Julie Sinnamon			
Contact Details	Queensland Government Chief Information Office (GovernmentICT@publicworks.qld.gov.au)			
Documentation Status	☐ Working Draft	☐ Consultation Release	☒	Final Version

Version History

Version Number	Date	Reason/Comments
0.0.1	15 Feb 2005	First draft
0.0.6	5 Mar 2005	Reformatted – bring control tables into body of document
0.0.7	8 Mar 2005	Revisions, added impact assessment table and flowchart
0.0.8	18 Mar 2005	Small revisions - sequencing
0.0.9	16 May 2005	Feedback from QSA
0.0.10	4 Aug 2005	Major Revision
0.0.11	19 Aug 2005	Minor revisions – sequencing
0.0.12	September 2005	Draft for consultation
0.1.0	22 September 2005	Released for Consultation
0.1.1	14 June 2006	Updated following consultation feedback
0.1.2 - 0.1.10	July – October 2006	Updated following additional consultation feedback, initial presentation to SI&ICT board and final review of consistency and accuracy.
1.0.0	3 November 2006	Endorsed version

Copyright

Copyright © The State of Queensland (Department of Public Works) 2005, 2006.

Copyright protects this material. Except as permitted by the Copyright Act, reproduction by any means (photocopying, electronic, mechanical, recording or otherwise), making available online, electronic transmission or other publication of this material is prohibited without the prior written permission of the Department of Public Works. Inquiries should be addressed to the Queensland Government Chief Information Office, Department of Public Works, GPO Box 2457, Brisbane Q 4001, Australia.

Acknowledgements

This framework was developed by the Information Security unit of the Queensland Government Chief Information Office, of the Queensland Department of Public Works, in consultation with the Queensland Government Chief Information Office Architecture and Standards Unit, the Queensland Government Information Security Steering Committee, Queensland State Archives, and the Security Planning and Coordination unit of the Department of the Premier and Cabinet.

Substantial parts of this framework were sourced from the Australian Government Protective Security Manual:2005, the Australian Government Information Technology Security Manual (ACSI 33):2006, the SSIO Better Practice Guide for Information Asset Classification and Control, and from material supplied by the Department of Justice and Attorney-General.

Legal

The Queensland Government owns or has a license to use the material published in this framework. The Queensland Government grants permission for the material comprising the Queensland Government Information Security Classification Framework or its supporting materials, to be copied, downloaded, printed or transmitted electronically.

If any of the material that forms part of the Queensland Government Information Security Classification Framework or its supporting materials is provided to a contractor or consultant employed by a department or agency of the Queensland Government, the employment conditions of the contractor or consultant must be such that the contractor or consultant will not be entitled to use the framework for any purposes other than the performance of consultancy services under that agreement. Clauses 9 and 11 of the standard consultancy contract used by Queensland Purchasing (available at http://www.qgm.qld.gov.au/contracts/Stand_Cond_Contract_Consultancy.doc) must be applied to all contractors or consultants so employed.

Models and frameworks used in the development of this framework and its associated parts may have been modified during the development effort to suit the needs of the Queensland Government. No guarantees can be made that those models and frameworks continue to serve their original intent or that they can be interpreted in the same way as the original. Any issues connected with the operation or interpretation of the models or frameworks should be referred to the Queensland Government in the first instance.

Table of Contents

1	Introduction	1
1.1	Purpose	1
1.2	Scope	2
1.3	Context.....	2
1.4	Implementation guidance.....	5
2	The Security Classification Schema.....	6
2.1	Public information	6
2.2	Official (non-public) information.....	7
2.3	National security information classification schema.....	7
2.4	Non-National security information classification schema.....	8
2.5	Security classification by domain.....	10
2.6	Security classification roles – Owner and User/Editor	11
3	The Security Classification Process	14
3.1	Identify information assets	14
3.2	Identify the owner of the information assets.....	15
3.3	Impact assessment of information assets	15
3.4	Determine the security classification of the information asset	18
3.5	Apply controls.....	19
3.6	Document security classified information assets in a register	19
3.7	Education and awareness	20
3.8	Maintain Security Classified Information Register – continuous review	20
4	General Controls	21
4.1	Need-to-know.....	21
4.2	Filing and markings.....	21
4.3	Clear desk policy.....	22
4.4	Reclassification of information.....	22
4.5	Information shared with external agencies.....	22
4.6	Disposal of information	23
5	Information Asset Security Classification Controls	24
5.1	UNCLASSIFIED.....	24
5.2	X-IN-CONFIDENCE (does not include CABINET-IN-CONFIDENCE)	25
5.3	PROTECTED	26
5.4	HIGHLY PROTECTED	27
6	Non-General Control Details.....	28
6.1	Discussing security classified information.....	28
6.2	Copying security classified information	29
6.3	Storage of security classified information and associated media	29
6.4	Electronic authentication and access controls	31
6.5	Audit logs.....	32
6.6	Email transmission	33
6.7	Facsimile transmission.....	33
7	References.....	34
7.1	Queensland Government legislation	34
7.2	Queensland Government standards.....	34
7.3	Australian Government standards	35
7.4	Australian standards	35
8	Glossary	36

1 Introduction

1.1 Purpose

Principle 3 of *Queensland Government Information Standard 18 – Information Security:2001 (IS18)*¹ addresses the requirement for Information Asset Classification and Control and requires that:

Agencies must define and publish a clear set of guidelines for the classification of sensitive information handled, created or received (in both electronic or paper-based formats) in accordance with sensitivity, confidentiality of content and business importance based on their legislative, regulatory and contractual obligations. To maintain a suitable level of protection for information, Agencies must identify and document major information assets and processes and assign responsibilities for the maintenance of their security.

This principle is expanded in the draft of the new version of *Queensland Government Information Standard 18 – Information Security:2006 (IS18)* which states that:

Agencies must implement policies and procedures for the security classification and protective control of information assets (in electronic and paper-based formats) which are commensurate with their value, importance and sensitivity. When addressing security classification and control policies and procedures, the agency must at a minimum ensure:

- *all major information assets used in agency operations are identified, documented and assigned owners for the maintenance of security controls;*
- *the security classification of all information is in accordance with Queensland Government Information Security Classification Framework;*
- *the control of all security classified information (including handling, storage, transmission, transportation and disposal) is in accordance with Queensland Government Information Security Classification Framework;*
- *security classification schemes do not limit the provision of relevant legislative requirements under which the agency operates; and*
- *disposal of public records is in accordance with legislative and regulatory requirements and with the agency's Retention and Disposal Schedules, as approved by the State Archivist or in accordance with the Public Records Act 2002.*

IS18 encourages a consistent approach for cross-Agency and inter-Governmental information sharing, by requiring that classifications for sensitive and classified information accord with the Queensland Government Information Security Classification Framework (QGISCF) (this document).

The QGISCF therefore enables agencies to meet their obligations of care and protection as outlined in *IS18*, by providing a standard process to allow agencies to evaluate their information assets and determine the appropriate level of security classification that should

¹ IS 18 URL: http://www.governmentict.qld.gov.au/02_infostand/standards/is18.pdf. As at endorsement of this framework, the 2006 edition of IS18 was in draft and not yet endorsed and hence subject to change from the wording reproduced here, with the 2001 edition remaining the formal version. This framework is intended to support both editions of IS18.

be applied, addressing the need for a consistent approach to dealing with the sensitivity and confidentiality of information across the Queensland Government.

The *QGISC* also specifies a schema for the security classification of information, and related controls which are in accord with the *Commonwealth Government Protective Security Manual (PSM)*².

By providing a standard approach to information security classification, the framework facilitates improved interoperability and consistency within Queensland Government agencies. The implementation of electronic service delivery has accelerated the need for a consistent approach to security classification, particularly as agencies seek to integrate services and information.

1.2 Scope

This framework provides a process and direction for determining the security classification of information assets³. Other security functions that are not directly related to the security classification of information are outside the scope of this framework. The framework is intended to address classification of information assets across all delivery mechanisms, including both on-line services and physical ‘over-the-counter’ services, and to apply to both electronically and non-electronically stored information. A single framework for all delivery mechanisms is vital because services and information are increasingly offered on multiple channels and across multiple agencies.

This document is intended for the use of staff within Queensland Government agencies. It will be of particular relevance to:

- information owners and user/editors⁴ who are responsible for classification and control of Queensland Government information assets;
- any people who are designing agency services such as business process specialists, service designers and system architects;
- business managers and service stakeholders;
- information security managers and auditors who may assess the security of services;
- records managers and others who have responsibility for managing classified information over time; and
- chief information officers and other ICT managers and staff responsible for the supply and operation of information systems.

1.3 Context

This framework has been developed to align with appropriate Queensland Government legislation and regulation, Australian Government standards, Australian Standards, and Queensland Government ICT Strategy and Policy. More information on some of these key inputs is provided below.

² More information on the PSM can be found at URL:
http://www.ag.gov.au/agd/WWW/protectivesecurityhome.nsf/Page/Protective_Security_Manual

³ See section 3.1 for more detail on information assets

⁴ See section 2.5 for more detail on information owners and users/editors.

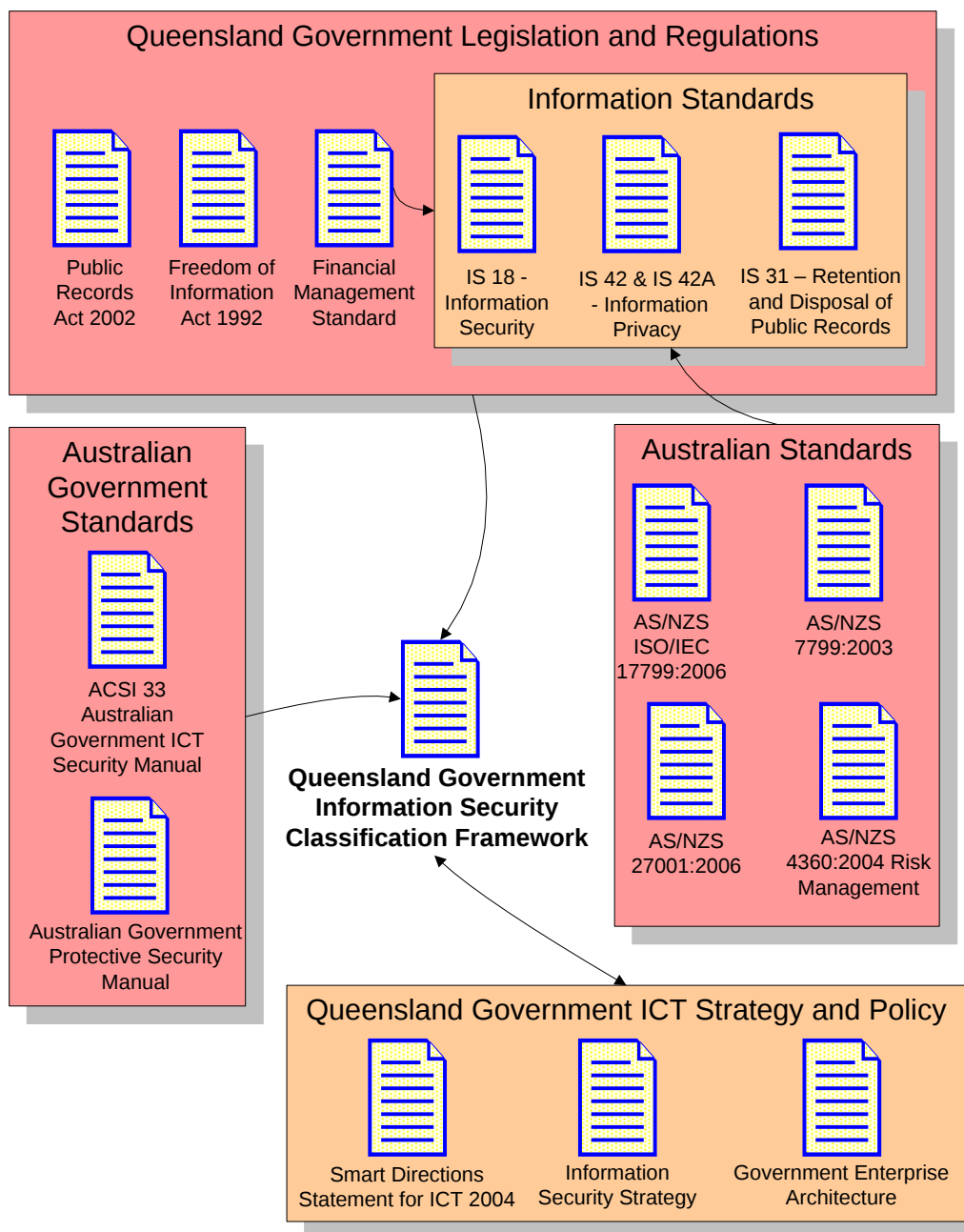


Figure 1: Context for QGISCF

1.3.1 Privacy Considerations

The Queensland Government has committed its agencies to the responsible and transparent collection and management of personal information that it collects from individuals. Limits on the transfer of personal information between agencies, other levels of government and the private sector are included within this commitment.

The principal instrument on data protection and privacy of personal information is the Australian Government's *Privacy Act 1988* and Queensland Government's privacy principles which are contained within *Information Standard 42: Information Privacy* and *Information Standard 42a: Information Privacy for the Queensland Department of Health* which are issued under the *Financial Administration and Audit Act 1977* and the *Financial Management Standard 1997*.

In the context of service delivery, privacy involves the appropriate control and use of personal information. The implementation of classification processes will have security and

privacy implications and a privacy impact assessment should be conducted when any new business processes are being developed, or during the modification of business process to ensure the privacy principles are followed.

1.3.2 Freedom of Information

Individual rights to access and amend personal information are the same as those contained in the *Freedom of Information Act 1992 (Qld)* and are processed under that legislation. The *Freedom of Information Act 1992 (Qld)* supersedes this classification framework. The security classification of information does not have a material effect on assessment of information for FOI purposes, nor on the implementation of the related Information Privacy Principles and other guidance provided by *Information Standard 42 and 42A – Information Privacy*.

1.3.3 Public Records Act

Information should be managed in accordance with the *Public Records Act 2002*. Provisions of this act relate to the management, retention and disposal of information and public access to records. This framework therefore has a strong linkage to the *Public Records Act*, and many of the provisions of management, retention and disposal provided within this framework are based on this act.

1.3.4 Queensland Government ICT Strategy and Policy

The *Smart Directions Statement for Information and Communications Technology*⁵ released in December 2004 sets the direction of ICT for all Queensland agencies. The *Queensland Government Information Security Strategy* has been developed by the Queensland Government Chief Information Office, to facilitate the implementation of the security components of the direction statement.

The *Information Security Strategy* is an initiative to improve Information Security both within an agency and in collaboration across government, whilst optimising resources used in achieving compliance.

The strategy is intended to create an Information security baseline across Queensland Government and a set of frameworks which will facilitate effective integration and interoperability of services both within the Queensland Government and with major partners including local and federal governments.

The context for information security classification as a process within the information security process framework is shown in the figure below.

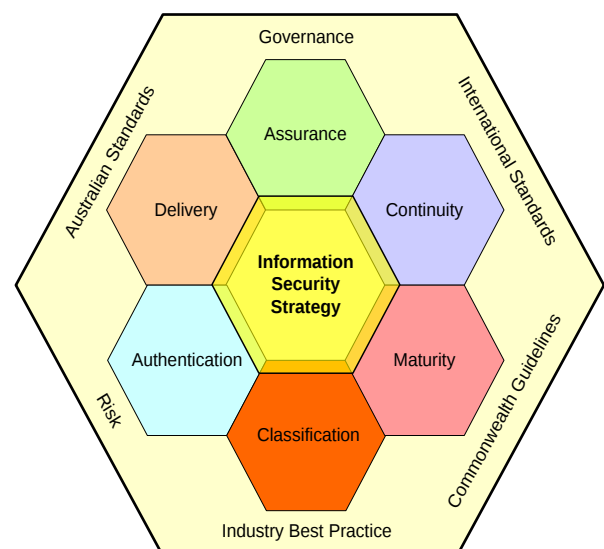


Figure 2- Queensland Government Information Security Framework

⁵ URL: http://www.governmentict.qld.gov.au/00_pdf/smartdirectionsstatement.pdf

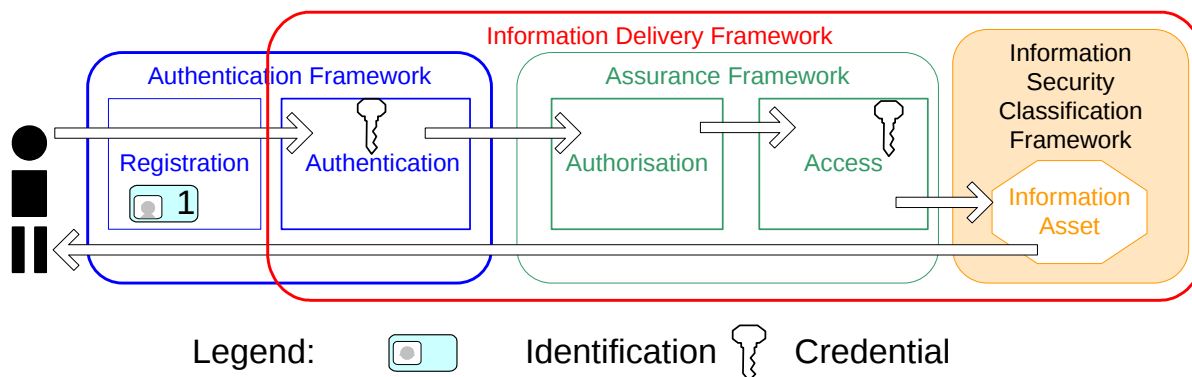


Figure 3: Information Security Classification context for the delivery of services

1.4 Implementation guidance

This framework should be used by all Queensland Government agencies to evaluate the security classification of their information assets. Ideally the *QGISC* should be applied to all information, and integrated into business processes to best protect information assets from unauthorised access, use, modification or destruction while maintaining high levels of performance and interoperability.

It should be noted that the impact assessment and evaluation criteria used in this framework is generic by design and therefore may not be suitable in its existing form for all agencies. It is therefore expected that agencies review the assessment to ensure it is useful and accurate for use within the agency before commencing with the security classification of information assets. Even where the impact assessment is appropriate, agencies will likely find it helpful to develop their own set of impact considerations (see section 3.3) with examples pertinent to agency business. This will help ensure staff applying the assessment process are provided with relevant and understandable guidance, resulting in better security classification decisions.

It is recognised that implementation will be progressive in nature. It is therefore recommended that *QGISC* be applied in the following order:

1. All new information assets should be evaluated against *QGISC* during their acquisition or implementation.
2. All information assets involved in existing information transfers either outbound from the agency or inbound.
3. Existing information assets should be evaluated when process changes occur to the collection or storage of the information, such as during the implementation of a new records or document management process or of a new information system. A particular driver for an implementation or review of security classification would be the implementation of a new process or system which enables the transfer of information beyond an agency's boundaries (for example to another agency or business partner).
4. The remaining existing information assets should be evaluated against *QGISC* based on an assessment of risk, with high risk information being considered a priority for evaluation.

Acknowledging that this framework can appear complex, the Queensland Government Chief Information Office will, wherever possible, assist agencies upon request with the assessment of information assets against this framework.

2 The Security Classification Schema

The section outlines the schema to be used for security classification of information within the Queensland Government. In order to maximise interoperability and eliminate the potential for confusion, this schema is the same as that used by the *Commonwealth Protective Security Manual:2005 (PSM)*.

Any information received or collected by, or on behalf of, the Government, through its agencies and contractors is official information. As it is a valuable official resource, official information:

- must be handled with due care and in accordance with authorised procedures
- must be made available only to people who have a legitimate ‘need-to-know’ to fulfil their official duties or contractual responsibilities, and
- must only be released in accordance with the policies, legislative requirements and directives of the Government and the courts.

Official information held within government typically falls into two broad categories:

1. Official information intended for public use / consumption; and
2. Official information which, because of the adverse consequences of unauthorised disclosure, requires appropriate controls to protect its confidentiality.

The following diagram provides a representation of the various security classifications of official Government information.

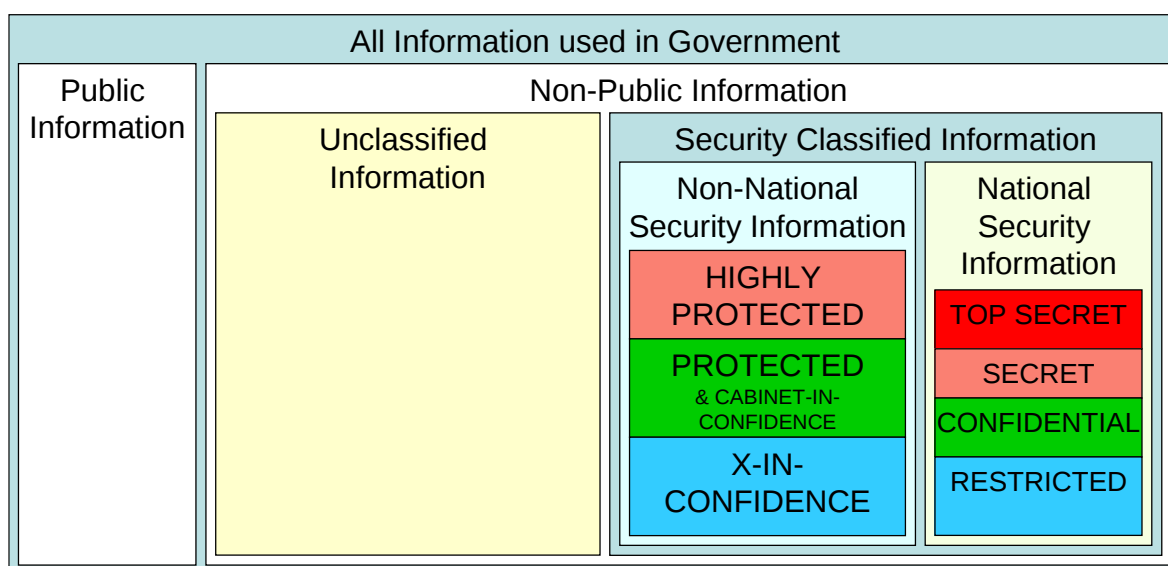


Figure 4: Government Information Security Classifications

2.1 Public information

Public information is that which has been authorised by the owner for public access and circulation, such as agency publications or web sites. Such information must be clearly labelled public to distinguish it from unlabelled unclassified information.

Whilst public information has no confidentiality requirements it is still important to ensure its accuracy and completeness (integrity) prior to its release. For example, information published on a web site must be protected from being tampered with or changed. This

information security classification framework does not discuss controls which ensure the integrity and availability of public information, and steps must be taken by agencies to ensure public information remains available and is not tampered with.

Some information intended for public consumption may have confidentiality requirements before its release (for example, Budget papers). In this case, the point at which the information will be reclassified to public must also be indicated⁶.

It should be noted that official information needs to be specifically classified as PUBLIC before it is released. Where information has not yet been classified, it should be treated as UNCLASSIFIED and not as PUBLIC.

2.2 Official (non-public) information

Official information that is not public can be further divided into:

Unclassified information

Information that does not need special security controls and comprises the bulk of the information resources used within government. Such information may remain unlabelled or be marked UNCLASSIFIED (indicating that an assessment has been performed). Employees must have authorisation from the information owner to release UNCLASSIFIED material to the public (which is in effect changing the classification of the information).

Security Classified Information

Security classified information requires additional controls according to the risk of compromise. The Commonwealth Protective Security Manual sets out two classification schema for security classified information according to whether or not the information affects national security. These classification schemas are:

- National Security Information
- Non-national Security Information

2.3 National security information classification schema

National security information is any official resource (including equipment) that records information about, or is associated with, Australia's:

- 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, that relate to significant political and economic relations with international organisations and foreign governments; or
- national interest, that relates to economic, scientific or technological matters vital to Australia's stability and integrity.

The national security classifications are: **RESTRICTED**, **CONFIDENTIAL**, **SECRET**, and **TOP SECRET**. People who are approved for access to information with these security

⁶ See section 3.4.1 for more information and examples.

classifications have been specifically trained and authorised to do so. People without this training and authorisation must not deal with nationally secured information.

Agencies must ensure that people who work for them are aware of the existence of national security and non-national security classifications even if they do not use both. It is essential that agencies respect the rule that information is classified by its originator. Information received from another agency cannot have the classification changed without the permission of the originating agency. The agencies receiving security classified information must provide the minimum security protection standards required for that level of classification.

TOP SECRET
SECRET
CONFIDENTIAL
RESTRICTED

Figure 5: National Security Classifications

This framework focuses on classification and control of non-national security information. Information security requirements for dealing with and managing national security information are complex and are not intended to be dealt with in any detail in this framework. Instead, a separate document has been developed to assist Queensland Government departments and agencies in complying with the minimum national standards for the protection of national security information. Please refer to “*The Queensland Policy and Procedures for the Protection of National Security Information*” for further guidance in this area. Whilst this document is unclassified, its distribution is limited to those agencies who access national security information on a routine basis or individuals who have a legitimate *need to know*.

You can obtain copies of this document from the Security, Planning and Coordination (SPC) Unit, Department of the Premier and Cabinet. Please contact the SPC on (07) 3405 6552, by email to security@premiers.qld.gov.au, or via post to PO Box 15185, CITY EAST QLD 4002.

2.4 Non-National security information classification schema

Non-national security information is any official information asset that requires increased protection and does not meet the definition of national security information. Most often this will be information about:

- government or agency business, 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 and so on;
- commercial interests, whose compromise could affect the competitive process and provide the opportunity for unfair advantage;
- law enforcement operations, whose compromise could hamper or render useless crime prevention strategies or particular investigations or adversely affect personal safety; or
- personal information, which is required to be protected under the provisions of the Government’s Privacy Principles, the *Public Records Act 2002*, or other legislation.

In addition to UNCLASSIFIED, there are three levels of non-national information security classifications which reflect the consequences of the compromise of the information. More information on X-IN-CONFIDENCE and CABINET-IN-CONFIDENCE is provided below.

HIGHLY PROTECTED	Information that requires a substantial degree of protection as compromise of the information could cause serious damage to the State, the Government, commercial entities or members of the public. Very little information belongs in the HIGHLY PROTECTED category and this security classification level should be used sparingly.
PROTECTED & CABINET-IN-CONFIDENCE	Information whose compromise could cause damage to the State, the Government, commercial entities or members of the public. This level of classification also includes CABINET-IN-CONFIDENCE (see 2.4.1 below). As a principle, most non-national security information would be adequately protected by the procedures given to information marked X-IN-CONFIDENCE or PROTECTED.
X-IN-CONFIDENCE	X-IN-CONFIDENCE information is information whose compromise could cause limited damage to the State, the Government, commercial entities or members of the public. Please note that X-IN-CONFIDENCE does not include CABINET-IN-CONFIDENCE, and all CABINET-IN-CONFIDENCE material should be treated as PROTECTED.
UNCLASSIFIED	Information which has been assessed for security classification and does not require one of the classification levels. It may be helpful to mark information with this classification level so that it is known that the assessment has been made. Information which has not been assessed is best marked Not-Yet-Security-Assessed or with some similar identification and should be treated as UNCLASSIFIED.

Table 1: Non-National information security classifications

2.4.1 CABINET IN-CONFIDENCE

The unauthorised and/or premature disclosure of matters contained in Cabinet documents (CABINET-IN-CONFIDENCE information) can be damaging to the public policy agenda and the government generally, and to the public interest. Unlawful disclosure of Cabinet-in-Confidence information may constitute an offence under the Criminal Code, Public Sector Ethics Act 1994 and constitute official misconduct under the Crime and Misconduct Act 2001.

CABINET-IN-CONFIDENCE material is to be treated as PROTECTED unless stated otherwise. The Cabinet Secretariat, within the Department of the Premier and Cabinet, facilitates the operation of Cabinet and its related processes, by providing advisory and administrative support to Ministers and departments. The primary guidance document to support these processes, including the handling of Cabinet material, is the Cabinet Handbook⁷.

⁷ Cabinet Handbook URL:

http://www.premiers.qld.gov.au/About_the_department/publications/policies/Governing_Queensland/Cabinet_Handbook/

2.4.2 X-IN-CONFIDENCE

The X-IN-CONFIDENCE label is intended to be modified by a notification of the subject matter in order to ensure correct handling and an easy appreciation of the ‘need to know’ requirement.

IN-CONFIDENCE: Can be used as a general label for in-confidence material where the need-to-know audience is not able to be clearly articulated in a label.

Examples of X-IN-CONFIDENCE labelling include:

- **STAFF-IN-CONFIDENCE:** Includes all official staff records where access would be restricted to HR personnel and nominated authorised staff. For example, personal files, recruitment information, grievance or disciplinary records.
- **EXECUTIVE-IN-CONFIDENCE:** Information associated with executive management of the entity that would normally be restricted to the executive and nominated authorised staff. For example, sensitive financial reports, strategic plans, Government matters and Staff matters, etc.
- **COMMERCIAL-IN-CONFIDENCE:** Procurement/contract or other commercial information such as sensitive intellectual property. For example, draft request for offer information, tender responses, tender evaluation records, designs and government owned research.
- **AUDIT-IN-CONFIDENCE:** Information related to audit activities where access would be restricted to officers of the Audit department or nominated authorised staff. For example, audit and risk reports which identify security and control weaknesses.
- **CLIENT-IN-CONFIDENCE:** Personal information about clients or held on behalf of clients which needs to be treated confidentially.

2.5 Security classification by domain

It is not practical to individually apply a full security classification process to every document, record or other information asset in use in an agency. Agencies should therefore consider an “information asset security domain”⁸ approach to information security classification. Information asset security domain classifications are not mandatory and should only be established where a logical grouping and standard impact assessment can be identified. It should also be noted that an individual information asset security classification will override any security domain classification.

An information asset security domain is a grouping of related information assets that share a security classification. Security domains allow a defined level of security classification to be automatically assigned to assets of the domain. This helps to ensure consistency and reduce owner and user/editor workloads. Domain security classifications must be approved by the information owner(s) responsible for the assets that the domain will apply to.

Some examples will help illustrate this concept. An example of an existing domain classification is cabinet documents, which are pre-determined as being CABINET-IN-

⁸ It should be noted that the information security domain concept being discussed here is not intended to be the same as other domains that may be specified through the Queensland Government GEA.

CONFIDENCE and are treated as PROTECTED information assets. Any new cabinet information does not need to be individually assessed, as it is clearly understood that it will be security classified as CABINET-IN-CONFIDENCE from the outset, and the appropriate controls applied. As another example, an agency may, through its information owner, determine that all employee records are to be security classified as IN-CONFIDENCE, and that all case files relating to a particular social service the agency provides are to be classified as PROTECTED because of the nature of the information they may contain.

The domain security classification scope will be determined by the ability to group information assets with similar impact assessment results. Often domains will be related to business functions such as HRM, Strategy or Procurement functions. Business classification schemes such as those developed for document and records management systems may be useful tools for identifying potential domain security classification areas.

Information asset security domain classification policies must also allow alternative security classification to be applied to assets. For example, an agency may consider the domain security classification for general Freedom of Information (FOI) applications to be IN-CONFIDENCE. However, if a FOI application involved HIGHLY PROTECTED assets, the classification of the FOI application may have to be increased.

Domain security classifications should be reviewed by agency information owners at least annually to ensure they remain appropriate.

2.6 Security classification roles – Owner and User/Editor

2.6.1 Information Owner

All information gathered and used by Queensland Government agencies is owned by the State of Queensland on behalf of The Crown. This responsibility is passed by the Governor to the Government, and on to the agencies of the Government. In practice, responsibility for ownership of information is usually vested with the Chief Executive Officer of the agency which holds the information on behalf of the Queensland Government, unless legislation, regulation or policy determines otherwise.

The information owner, therefore, is the recognised officer who is identified as having the authority and accountability under legislation, regulation or policy for one or more information assets. Information owners define the policy which governs the information assets of an agency, including determining the security classification of information assets.

In order to ensure due attention is able to be applied to this role, it is standard practice for CEO's to further delegate the responsibilities and authority of their role as information owner to another senior staff member or members. When this occurs, it is important that the scope of delegated responsibilities should be clear and formally documented so that accountability and

EXAMPLES OF INFORMATION OWNERS

The Transport Operations (Maritime Safety) Act 1994 requires the Chief Executive of Maritime Safety to develop maritime safety strategies. Therefore, the Chief Executive of Maritime Safety is responsible for setting classification requirements for maritime safety strategies.

The Survey and Mapping Infrastructure Act 2003 requires the nominated chief executive to maintain a state wide digital cadastral data set. The nominated chief executive is also responsible for determining classification requirements.

audit requirements are able to be met and confusion as to who is the appropriate delegated information owner is avoided⁹. Information ownership should generally be assigned as part of a role, rather than being personally assigned to a particular individual. In this way, the responsibility is continued when individuals move roles.

Where information ownership is to be delegated to more than one individual, it is advisable that these individuals have clear domain responsibilities. For example, the Director of Human Resources may be assigned as information owner for all human resource related information assets. If at any time an information asset is not able to be clearly assigned to a delegated information owner, the CEO will be required to make the security classification determination.

The security classification responsibilities of an information owner include:

- ensuring agency policy and procedures are in place to support security classification of information assets;
- setting and ratifying any security classifications for information assets or domains of information assets¹⁰;
- conducting an annual review of security classified information assets;
- ensuring information asset security domain classifications are reviewed at least annually or when changes have occurred to the internal controls used to protect the information assets;
- ensuring that Service Level Agreements or Operating Level Agreements between agencies and/or private entities managing agency information assets include appropriate service levels and targets relating to information being accurately security classified and managed in accordance with the controls described in this framework and/or other relevant agency policy;
- providing resources to support agency security classification and control requirements; and
- approving classifications or re-classifications of information assets as recommended by user/editors¹¹.

2.6.2 Information User/Editor

Anyone who uses, edits, modifies or originates information can be considered an information user/editor. Information user/editors are required to implement relevant policy of an organisation regarding the use of information, including applying the controls specified by the security classification of information.

In many cases, where a user is creating new information, or receives information into the agency from another source which has not been security classified, the user will be required to make the initial recommendation as to the security classification of the

⁹ It should be noted that current practice is that some agencies use the name “delegated information owner” for this final responsible officer, some simply use “information owner”, and take it as read that ownership is delegated from the highest level of an organization on behalf of the state, and some use the term “information custodian” to refer to the officer who has delegated responsibility to determine information policy including information security classification. Within this framework, references to “information owner” can be read as including “delegated information owner”.

¹⁰ Domain classifications cover a group of similar information – for example, HR information may default to being classified as “in-confidence”. If domain classifications are used, they should be approved by the owner to ensure accountability for the decision.

¹¹ Information assets that are classified as PUBLIC, X-IN-CONFIDENCE, PROTECTED or HIGHLY PROTECTED incur substantial management and control costs. Their classification should be ratified by the owner to ensure resources and support is available to manage the assets appropriately and minimise the risk of inappropriate exposure.

information asset, but the information owner in the receiving agency retains the approval responsibility for classifying the information

The security classification responsibilities of a user/editor include:

- ensuring appropriate controls are applied to security classified information; and
- where information is being dealt with which has not already been security classified, making an initial recommendation for a security classification following the process outlined below.

The process for determining an appropriate security classification for information not already classified is shown diagrammatically in Figure 6, and expanded in words below.

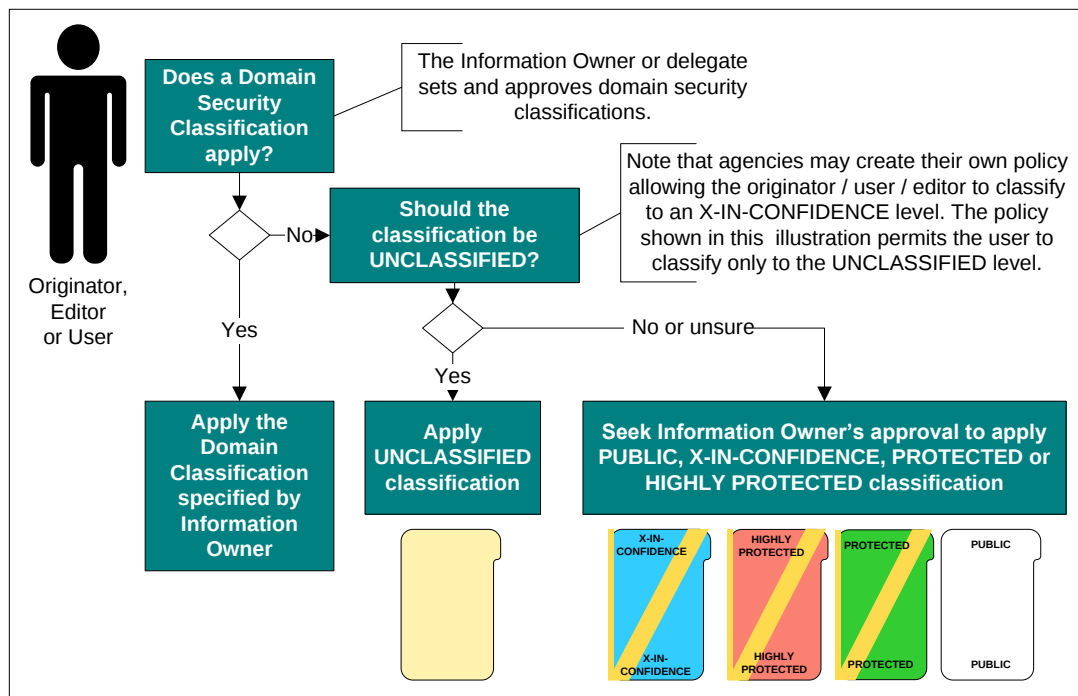


Figure 6: User/Editor Classification Process

The process is:

- User/Editor creates or receives new information which is not yet security classified.
- User/Editor determines if a domain security classification exists for this information asset type (eg is this a known information asset type such as a HR record, that has a pre-defined security classification).
 - If a domain security classification does exist, apply it.
 - If it does not, proceed to next step.
- The User/Editor needs to consider the security classification level which should apply. Agencies will need to have their own policy which covers what levels of security classification a User/Editor can apply without reference to the information owner. Suggested approaches are to allow user/editors to apply UNCLASSIFIED only, or to allow users to apply either UNCLASSIFIED or IN-CONFIDENCE security classifications (the former being illustrated in Figure 6).
 - If the user, using the process outlined in Section 3 of this framework, determines that the security classification of the information asset is one which agency policy allows User/Editors to determine, they may apply that security classification without further reference to the information owner.
 - If the user thinks that the security classification is likely to be one which they do not have authority to apply, or they are unsure, they should refer to the information owner for a determination to be made.

3 The Security Classification Process

This section provides detail on the security classification process, which is described diagrammatically below. It is necessary to ensure that the process is understood to be a living process, that is, that information security classification of information needs to be periodically and regularly reassessed, and that the application of this process on a one-off basis will not provide the required protection of information.

Each of the steps identified below is expanded in more detail in the following sub-sections.

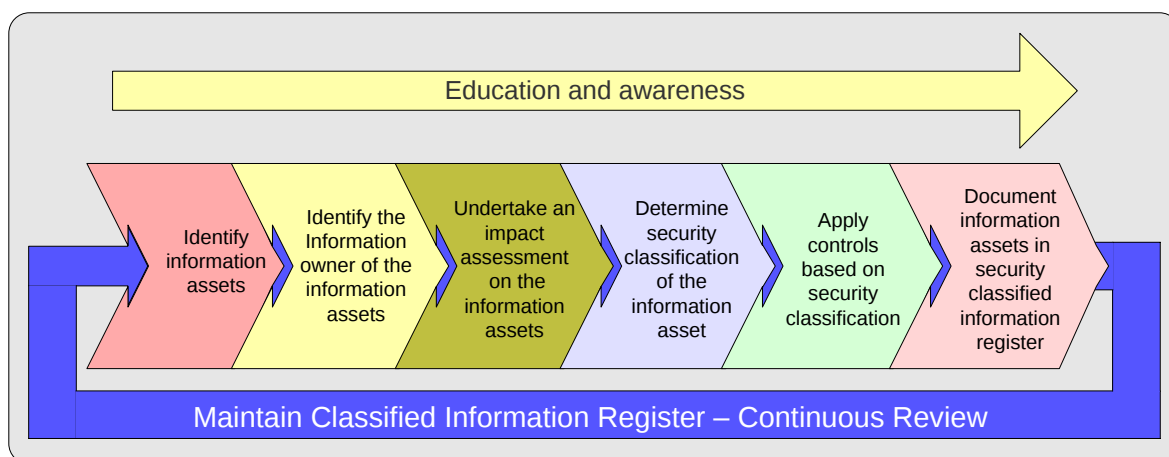


Figure 7: Information Security Classification process

3.1 Identify information assets

For the purposes of this framework, **information assets** are defined as information in any form. As such, information assets include documents, files, and electronic data.

Some examples of information assets include, but are not limited to:

- **employee related information** including employee records, job applications, and records of interview;
- **procurement records** such as draft specifications, tender evaluations, contracts, vendor pricing details, and performance reports;
- **corporate documentation** such as corporate policies, strategic plans, ministerial and other correspondence, briefing notes, legal advice, business, financial and audit reports, guidelines, system documentation, user manuals, training material, operational and support procedures, business continuity plans, system architecture drawings, and risk analyses; and
- **client information** including service level agreements, memoranda of understanding, service contracts, client contact records.

Information spanning multiple media types or formats must ensure classification requirements are applied to all types or format, to ensure overarching classification control is maintained.

If any information assets exist that are not stored in paper based or electronic formats (such as photographs or test samples), they should still be classified using the *QGISCF* but will require additional agency policies to ensure consistent evaluation and application.

Please note that information asset is not used within this framework to refer to the technology which is used to store, process, access and manipulate information, which is

more properly described as **ICT (Information and Communication Technology) assets**. ICT assets which are not considered information assets include:

- **software** including application and system software, development tools and utilities, and the associated licences; and
- **physical assets** such as computing equipment, storage media (CDs, DVDs, tapes and disks), and power supplies, air conditioners and other technical equipment which may impact the confidentiality, availability, or integrity of information resources.

3.2 Identify the owner of the information assets

Each agency is responsible for ensuring that information has a security classification and is authorised by the information owner. Information should be classified by the information owner or delegate at the earliest possible opportunity and as soon as the originator or owner is aware of the sensitivity of the information asset.

In the case of information externally generated, and not otherwise classified, the agency officer who receives the information should approach their own agency information owner or delegate to classify the information and guide its control within the agency (see section 2.6.2 for more detail on the User/Editors role in security classification and section 4.5 for more on receiving external information).

3.3 Impact assessment of information assets

When determining the correct information security classification level for an information asset or domain, a range of considerations need to be made. Where information can be security classified according to legislation, regulation, policy, contractual or other pre-determined means, it should be so classified. For example, breach of proper undertakings to maintain the confidentiality of information provided by third parties and breach of statutory restrictions on the management and disclosure of information need to be considered, and these may influence the final security classification level.

For agency information for which the security classification cannot be so determined, the following Impact Assessment Matrix should be used to assess the impact of the information asset being compromised, and to guide the determination of the information security classification. It should be noted that this matrix is intended as a guide only, and the impact types and their evaluation may need modification to suit individual agencies and their business processes. Some agencies will find a need to add additional impacts, and others may find the matrix can be simplified by removing irrelevant impacts. Examples of other impacts that could be added include threats to state security, impact on legal proceedings, or impact on the State Government's relationship with other governments. Some agencies may also find it useful to use existing risk management terms for the Impact Severity scale (None/Negligible, Minor, Moderate, High, Very High) providing these alternate terms do not change the essence of the impact assessment.

It should also be noted that the presentation form of information may affect its security classification, and therefore the presentation of the information needs to be taken into account during this assessment. For example, a high resolution satellite image may require an IN-CONFIDENCE level of information security classification, but a low-resolution version of the same image may be able to be classified as PUBLIC. Likewise, some documents may be produced in both a public and a modified security classified form. It is important to note that information which is evaluated to have no impact should not automatically be classified as PUBLIC, but may be considered suitable for this

classification. UNCLASSIFIED is the most appropriate default classification, and PUBLIC should only be used when there is a specific reason for the information to be published and made available to the public.

IMPACT Type	Severity				
	Lowest				Highest
Impact Severity	None / Negligible	Minor	Moderate	High	Very High
Risk to Individual safety	None / Negligible			Any risk to personal safety	Threaten life directly
Distress caused to any party	None / Negligible		Short term distress	Limited long term distress	Substantial long term distress
Damage to any party's standing or reputation	None / Negligible		Short term damage	Limited long term damage	Substantial long term damage
Inconvenience to any party	None / Negligible	Minor inconvenience	Minor inconvenience	Significant inconvenience	Substantial inconvenience
Public order	No / Negligible Impact		Measurable Impact	Prejudice	Seriously prejudice
Inappropriate release of personally or commercially sensitive data to third parties	No or Negligible Impact	Minor impact	Measurable impact, breach of regulations or commitment to confidentiality	Release of information would have significant impact	Would have major consequences to a person, agency or business
Impact on Government finances or economic and commercial interests	No or Negligible Impact		Cause financial loss or loss of earning potential	Work Significantly against	Substantial Damage
Financial loss to any client ¹² of the service provider or third party	None / Negligible	Minor loss	Moderate loss	Significant loss	Substantial loss
Financial Loss to Agency / Service Provider	None / Negligible	Minor < 2% of monthly agency budget	Moderate 2% – < 5% of monthly agency budget	Significant 5% – < 10% of monthly agency budget	Substantial ≥ 10% of monthly agency budget
Threat to government agency's systems or capacity to conduct their business ¹³	No or Negligible threat			Agency business or service delivery impaired in any way	Agency business halted or significantly impaired for a sustained period
Assistance to Crime or impact on its detection	Would be of no or negligible assistance or hindrance to detection of unlawful activity		Prejudice Investigation or facilitate commission of violations that will be subject to enforcement efforts	Impede investigation or facilitate commission of serious crime	Prevent Investigation or directly allow commission of serious crime
Impact on development or operation of major government policy	No or Negligible Impact	Minor impact	Impede effective development or operation	Seriously Impede	Substantially Impede

	↓	↓	↓	↓	↓
SECURITY CLASSIFICATION	Consider for PUBLIC or UNCLASSIFIED	UNCLASSIFIED	X-IN- CONFIDENCE	PROTECTED	HIGHLY PROTECTED

Table 2: Impact assessment matrix

¹² In order to assist in the determination of the appropriate level of impact, the following is suggested: Min or <\$50, Moderate \$50- <\$200, High \$200 - <\$2000 and Very High >=\$2000. These figures are guidelines only, and are based on an "average" individual. Where the client is known to be a corporation of other similar entity, these figures would need to be adjusted to something more akin to the figures used for financial loss to the service provider. If multiple clients will suffer the loss, the impact level should be adjusted accordingly to reflect the total losses to clients.

¹³ The period here may vary from agency to agency – some agencies may be able to endure a halt in business for a number of days without serious impact on the government or society. Others more directly involved in public safety and similar services would be less tolerant of outages.

To provide some assistance in completing the impact assessments, the following table provides examples of considerations agencies may make when assessing each impact type. Agencies may have other considerations when assessing impacts, and it may be useful for agencies to develop their own guidelines as to the considerations which may apply to each impact type and to use those guidelines for their assessment process.

Impact Type	Possible considerations
Risk to party's safety?	Consider any risk of any injury or impact on safety at all, as well as the possibility of loss of life. An example could include release of names or locations of under-cover officers, people under protection orders, etc
Distress caused to any party?	From the client's or public's point of view, distress could be caused by many things, including the release of private information. From a service provider's point of view, potential impacts could include stress impacts on employees and possible loss of jobs or major reorganisation forced by the inappropriate release of information.
Damage to any party's standing or reputation?	Issues to consider include potential for adverse publicity, either locally or wider, and the potential to damage occurring to either the service provider's or client's ongoing reputation. If inappropriate access to information was granted etc, would it be of interest to the media?
Level of inconvenience to any party?	Consider factors such as releasing information which could lead to identity fraud being perpetrated.
Public Order	Need to consider whether disclosure of information could pose a threat to community relations and public order. This may occur when information is released that can cause "alarm" in a way that then results in damage to public order. An example would be disclosure of an offender's identity or whereabouts where the community could then react and disturb public order.
Inappropriate release of personally or commercially sensitive data to third parties?	Would disclosure of information which should not be made public have an impact on any party, or would it violate legislative or regulatory guidelines such as information privacy principles? Examples include medical records and other personal information and commercially sensitive information that could impact on current or future business.
Impact on Government finances or economic and commercial interests	Would disclosure of information result in financial or economic consequences to government. Release of information may result in financial gain or loss. Disclosure of planning decisions which could result in changing valuations would be an example
Financial Loss to any client of the service provider or third party	Consider this from the service providers perspective - what losses could they incur? Considerations include possibility of fraud, a party illegally transferring money, a party gaining control of assets they don't legally own (eg by using the provided information to establish an identity which is not theirs, and then changing ownership details), etc.
Financial Loss to service provider?	Consider this from the service providers perspective - what losses could they incur? Considerations include possibility of fraud, a party illegally transferring money, a party gaining control of assets they don't legally own (eg by using the provided information to establish an identity which is not theirs, and then changing ownership details), etc.
Threat to government agencies' systems or capacity to conduct their business?	Would inappropriate release of this information have the potential to reduce or prevent an agency or external party conducting their business? For how long would this reduction / prevention last?
Assistance to serious crime or hindrance of its detection?	Would release of this information have the potential to assist in the conduct of a crime or terrorist activity? This could include release of information enabling the planning of a crime or terrorist activity, or the creation of a false identity.
Impact on development or operation of major government policy	Would inappropriate disclosure cause embarrassment to government in the stages where policy is being formulated or implemented? The impact may be that a major policy initiative will not proceed.

Table 3: Impact considerations

3.4 Determine the security classification of the information asset

The highest security classification level determined by the impact assessment must be applied to that asset. For example, an analysis of a particular information asset may show the following impact assessment:

Consequence	Impact Severity
Risk to Individual safety	None
Distress caused to any party	High
Damage to any party's standing or reputation	High
Inconvenience to any party	Moderate
Public order	Minor
Inappropriate release of personally or commercially sensitive data to third parties	Minimal
Impact on Government finances or economic and commercial interests	Minor
Financial loss to any client ¹⁴ of the service provider or third party	None
Financial Loss to Agency / Service Provider	Minimal
Threat to government agency's systems or capacity to conduct their business	None
Assistance to Crime or impact on its detection	None
Impact on development or operation of major government policy	Moderate

Table 4: Example impact assessment

In this example, the highest impact identified is High, and hence the information should be classified as PROTECTED.

As mentioned earlier, other agency, regulatory or legislative issues including privacy, freedom of information and the public records act may also impact on the classification of the information, and need to be considered at this point.

3.4.1 Limiting the duration of the classification

When an information asset is classified, it may be possible to determine a specific date or event, after which the consequences of compromise might change. An event may trigger an increase in the sensitivity of the information, for example a HR form may become "STAFF-IN-CONFIDENCE (when complete)" or, as is often the case, the sensitivity of the information may decrease over time, for example budget documents that may be "BUDGET-IN-CONFIDENCE (until tabled on 15 Jun 04)". Some information may require increased protection because it is under embargo until a specific public policy statement,

¹⁴ In order to assist in the determination of the appropriate level of impact, the following is suggested: Minimal <\$50, Minor \$50- <\$200, Significant \$200 - <\$2000 and Substantial >=\$2000. These figures are guidelines only, and are based on an "average" individual. Where the client is known to be a corporation of other similar entity, these figures would need to be adjusted to something more akin to the figures used for financial loss to the service provider. If multiple clients will suffer the loss, the impact level should be adjusted accordingly to reflect the total losses to clients.

after which it is in the public domain. In the event that a future date cannot be determined, it is essential to ensure that the date the information was created or classified is noted (for example in the Security Classified Information Register), so that this can be used for future assessment of classification levels, and for Freedom of Information purposes.

3.5 Apply controls

The following sections of this framework provide details of appropriate controls which should be applied to ensure that protection is given to the information commensurate with the level that has been determined.

3.6 Document security classified information assets in a register

Organisations should establish and maintain a Security Classified Information Register (SCIR) to record the security classification of each information asset. This register is ideally maintained in a central location and should cover all security classified information assets of an agency, so it can be readily accessed and referred to by the Chief Executive and other officers. The security classified information register may well be a sub-set of an overall agency information asset register, and may be established using exist asset control or document and records management systems.

It should be noted, that whilst highly desirable for X-IN-CONFIDENCE and PROTECTED information, it is only mandatory to record HIGHLY-PROTECTED information assets within the security classified information register.

As a minimum, for the purposes of this framework, the register should include:

- name or unique identifier of asset or group of assets (e.g. a unique file number or name, data base name, etc);
- description of information asset (i.e. what is it about);
- location of information asset;
- information owner;
- security classification of the information asset;
- date of security classification with details of the authority of the classifier (eg who approved the classification);
- reason for the security classification of the information asset (particularly important to support review and reclassification of the information asset at a later time - should include legislative, regulatory, policy or other reference where applicable, or a copy of the impact assessment made); and
- date to review security classification (if known).

Additionally, the following information is desirable for HIGHLY PROTECTED information assets, and is desirable for other classifications:

- users and usage of the information;
- number of copies in circulation and their location; and
- disposal details where information has been disposed of.

It should be noted that electronic document and records management systems (eDRMS) generally contain functionality to record classification metadata for information they manage, and may be capable of automatically populating and maintaining a security classified information register for the information they control.

It should also be noted that the security classified information register is, in itself, an information asset, and, with due care as to the information recorded in it, such an inventory of information assets would normally have a default classification of SECURITY-IN-CONFIDENCE because of the information it provides on other security classified information. Agencies should make their own assessment of the security classification of the SCIR implement appropriate controls.

For HIGHLY PROTECTED information assets, at irregular intervals, the information owner must either conduct, or arrange for a nominated officer to conduct, a spot check of a small sample of HIGHLY PROTECTED information assets to ensure that these are accounted for and are being handled, stored, etc, in accordance with the minimum standards set out in this framework. It is good security practice to conduct a similar spot check of other security classified files at irregular intervals.

The Security Classified Information Register itself should be reviewed and maintained at least annually.

3.7 Education and awareness

The ongoing education and awareness of all employees in the importance of security classifying information, is critical to the success of the overall agency security environment. The agency should ensure that all employees who create, processes, or handle security classified information have a clear understanding of the agency classification policies and procedures and of their responsibilities.

Education and awareness programs will likely vary across an agency and between agencies and depend on the type of work and types of information dealt with. For example, where staff are not expected to deal with PROTECTED or HIGHLY PROTECTED information, training can concentrate on general awareness and the controls and processes surrounding the IN-CONFIDENCE classification and how to obtain assistance if they do need to handle the other classification levels.

3.8 Maintain Security Classified Information Register – continuous review

As environments and circumstances change, information owners may choose to review security classifications to ensure that the protection being afforded the information is cost-effective and commensurate with the level of risk.

Security classification makes records more expensive to handle, store and transfer, so ensuring the information security classification of information is appropriate is important. This may require de-classifying information that is no longer sensitive, or increasing the classification where the consequence of compromise has changed.

Information must be declassified or downgraded when protection is no longer required at all or is no longer required at the original level. If an information User/Editor believes that an information asset has been incorrectly security classified, they must advise the information owner who may consider the need to reclassify the information.

Information Owners should use the SCIR to annually review the security classification of information assets.

4 General Controls

As well as the specific controls contained in the following sections, the following controls need to be applied to all information, regardless of the security classification of the information.

4.1 Need-to-know

The need-to-know principle requires that information held by an agency should only be available to those who need to use or access the information to do their work. The dissemination of information must be no wider than is required for the efficient conduct of business and it is the personal responsibility of all those who use or access official information, including unclassified information, to apply the need-to-know principle to their duties. It is the responsibilities of agencies to determine need-to-know designations for staff. In relation to personal information, this is subject to the Information Privacy Principles in *IS42* and *IS42A* and any confidentiality provisions contained in the legislation of agencies.

Agencies typically implement a need-to-know approach to information access through a combination of access control on applications and the implementation of both individual and work-unit based security mechanisms for file servers. It should be noted that the need-to-know principle may not inhibit access to information under legislation such as the *Freedom of Information Act 1992*.

4.2 Filing and markings

Security classified documents should be filed with appropriate “wrapper folders” or file covers. It should be noted that the coloured folders identifying security classification levels should be used as wrappers on physical documents or files, and are not intended to replace existing storage folders that may be used to track file movements or other information.

The *Protective Security Manual* specifies standard file colours as indicated in table 5. The recommended stripe colour is Pantone Process Yellow-2U. The stripe should run diagonally across the front and on the spine (see section 5 for illustrations).

Security Classification	File Colour
TOP SECRET	post office red
SECRET	salmon pink
CONFIDENTIAL	Green
RESTRICTED	blue or buff
HIGHLY PROTECTED	salmon pink plus stripe
PROTECTED	green plus stripe
X-IN-CONFIDENCE	blue or buff plus stripe

Table 5: PSM standard file colours

Generic Queensland Government coloured and printed folders have been sourced by some agencies and are therefore available for purchase. Where agencies have other requirements that preclude the use of the standard colour file covers, agencies should ensure that an appropriate standard is adopted within the agency. File cover sheets should also be used for all physical files, and standard cover sheets have been developed in support of this framework.

The PSM recommends that the security classification should be in capital letters, in bold text, and of a minimum height of 5mm, preferably at the centre of the top and bottom of each page. Additionally where possible it is preferable for the markings to be in red (ARIAL, 20 point, bold and red is an appropriate format). Page numbering of the form “Page n of x” is desirable for all classifications and mandatory for HIGHLY PROTECTED.

Markings for PUBLIC and UNCLASSIFIED documents should also be in capitals, bold and red, but may be in a smaller size font if required. Because of the possibility of confusion with UNCLASSIFIED, an acceptable markings for UNCLASSIFIED documents are “UNCLASSIFIED”, “INTERNAL-USE-ONLY”, or a combination “UNCLASSIFIED–INTERNAL-USE-ONLY”. A domain can also be added if this is appropriate and would assist such as “AGENCY-INTERNAL-USE-ONLY” or “GOVERNMENT-INTERNAL-USE-ONLY”.

4.3 Clear desk policy

A clear desk policy requires that classified official information is secured when workstations are unattended and that unauthorised people are not able to access any electronic material, system or network to which the user had been connected. For long periods this would mean ‘logging off’ from computer systems, but for shorter periods a screen saver with password or some similar desktop locking mechanism may be adequate.

At close of business, a workplace lock-up procedure should require that personnel:

- quit all systems and networks and, where possible, shut down workstations;
- ensure that there is no security classified information left unsecured;
- ensure there is no security classified information in waste-paper bins and that information is instead disposed of correctly;
- ensure that electronic media storing security classified information are secured;
- clear whiteboards and other displays of any security classified information;
- secure vaults and containers holding security classified material;
- ensure windows and doors are locked; and
- ensure that keys to containers holding security classified information are secure.

4.4 Reclassification of information

Employees should not change the classification of information unless this action is a formal part of the reclassification process approved by the information owner. Reclassification of information assets should be performed in accordance with the standard classification process outlined in this framework and other agency specific classification processes.

4.5 Information shared with external agencies

Where agencies are required to handle security classified information from external agencies, the information must:

- Retain the security classification of the forwarding agency;
- Be managed according to that agencies information security classification scheme and policies or in line with a Memorandum of Understanding or Service Level agreement established between the agencies. The originating agency is responsible for ensuring that its information will be properly protected.
- If a MOU or other agreement has not been made, the information must, as a minimum, be handled in accordance with this framework.

4.6 Disposal of information

Section 26 of the *Public Records Act 2002* provides for the disposal of public records and applies to records created and maintained in any format. The Public Records Act defines disposal of a record as including:

- Destroying or damaging the record, or part of it; or
- Abandoning, transferring, donating, giving away or selling the record, or part of it.

Information Standard 31 - Retention & Disposal of Public Records (IS31)

Information Standard 31 - Retention & Disposal of Public Records (IS31) requires that the disposal (including the destruction, sale or transfer) of records can only be performed with the written authorisation of the State Archivist. Public authorities must develop and implement formal disposal schedules authorised by the State Archivist and implement disposal processes, to ensure the legal, systematic, and consistent disposal of records no longer required for business, accountability or cultural purposes.

Sanitising and Disposal of media used to store information

The following media cannot be sanitised and should be destroyed if they contain or may have contained classified information:

- Microfiche and microfilm;
- Optical discs, including CDs and DVDs;
- Printer ribbons; and
- Programmable read only memory (PROM) and read only memory (ROM).

Other media including various forms of erasable or alterable PROM (EPROM), laser printer and photocopier drums, and magnetic media such as hard disk drives may be sanitised for reuse by wiping or by using a suitable degaussing tool. Sanitisation of magnetic media by erasure should be performed using specifically designed security erasure software to effectively wipe the contents of electronic storage media.

Methods of destruction

Security classified material may be disposed of by:

- pulping: transforming used paper into a moist, slightly cohering mass, from which new paper products will be made.
- burning: (in accordance with relevant environment protection restrictions).
- pulverisation: using hammermills with rotating steel hammers to pulverise the material.
- disintegration: using blades to cut and gradually reduce the waste particle to a given size determined by a removable screen.
- shredding: using cross-cut shredders. Where the disposal method is shredding, classified material should be destroyed using a cross-cut shredder that reduces waste to a particle size of 2.3mm x 25mm or less (B Class Shredder).

Garbage and recycling

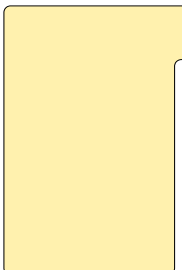
Security classified information should not be recycled or discarded in the agency's general garbage unless it has already undergone some form of appropriate destruction, such as shredding.

Any decision to dispose of security classified waste using an authorised disposal company should be determined in the context of sound risk management and with the authority of the information owner.

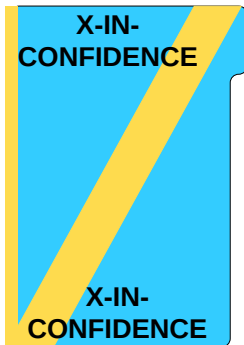
5 Information Asset Security Classification Controls

This section contains summary details of the controls relevant for the various security classification levels. The following section provides some more details on some of these controls.

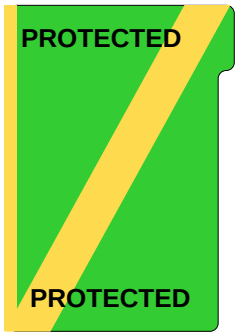
5.1 UNCLASSIFIED

Plain folder 	UNCLASSIFIED information is official information that is not in the public domain, but does not otherwise need to be classified. The unauthorised disclosure or compromise of UNCLASSIFIED information may undermine public confidence in Government operations. UNCLASSIFIED information is information which still needs to be protected and controlled, and is not to be considered PUBLIC information. Official information needs to be specifically classified as PUBLIC before it is released. It may be helpful to mark information with this classification level so that it is known that the assessment has been made. Information which has not been assessed is best marked Not-Yet-Security-Assessed or with some similar identification and should be treated as UNCLASSIFIED. UNCLASSIFIED information may be marked as INTERNAL-USE-ONLY, AGENCY-INTERNAL-USE-ONLY, GOVERNMENT-INTERNAL-USE-ONLY or UNCLASSIFIED.		
Preparation and Handling Markings Not required, though helpful in distinguishing UNCLASSIFIED information from information that has not been classified. Page Numbering Optional, but generally helpful. Filing: File in accord with normal records management practices. SCI Register Not Required. User Auditing Log in, log out, failed attempt. Printing No special requirements.	Removal from workplace, and monitoring Removal of file or document only on a basis of need. Monitoring None required.	Copying and storage Copying To be kept to a minimum in accord with operational requirements. Storage May be stored in unsecured compactus or cabinet. Electronic Storage Common access drive or directory.	
	Discussing Unclassified Information Meetings No restriction but basis of 'need-to-know' Telephone and video conference May be passed in the clear (unencrypted) over communications systems.		
Manual Transmission Within a single location May be passed uncovered by hand. Passed by internal mail in a use again envelope. Between locations Passed by internal mail in a use-gain envelope. Passed by external mail in an opaque envelope.	Electronic Transmission Data transmission Basis of 'need-to-know'. May be passed by data transfer using internal or external networks including the internet. email Basis of 'need-to-know'. May be passed by email using internal or external networks including the internet. Fax Unclassified information may be passed in the clear (unencrypted) by fax.	Archive & Disposal In accordance with authorised retention and disposal schedule issued under Section 26 of the Public Records Act 2002. Paper waste Drafts, working papers and copies may be recycled. Drafts, working papers and copies may be discarded with general paper waste. Electronic Media & equipment Media may be reused or disposed of as per paper waste.	

5.2 X-IN-CONFIDENCE (does not include CABINET-IN-CONFIDENCE)

Blue folder 	Information whose compromise could cause limited damage to the State, the Government, commercial entities or members of the public, including: • cause distress to individuals or private entities; • cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or private entities; • prejudice the investigation or facilitate the commission of crime; • breach undertakings to maintain the confidentiality of information provided by third parties; • impede the effective development or operation of government policies; • breach statutory restrictions on the management and disclosure of information; • disadvantage the Government in commercial or policy negotiations with others; or • undermine the proper management of the public sector and its operations. This protective marking is accompanied by a notification of the subject matter which alludes to its audience and the need-to-know principle. Examples include: STAFF-IN-CONFIDENCE Includes all official staff records where access would be restricted to HR personnel and nominated authorised staff. For example, personal files, recruitment information, grievance or disciplinary records. EXECUTIVE-IN-CONFIDENCE Information associated with executive management of the entity that would normally be restricted to the executive and nominated authorised staff. For example, sensitive financial reports, strategic plans, Government matters, Staff matters, etc. COMMERCIAL-IN-CONFIDENCE Procurement/contract or other commercial information such as sensitive intellectual property. For example, draft request for offer information, tender responses, tender evaluation records, designs and government owned research. AUDIT-IN-CONFIDENCE Information related to audit activities where access would be restricted to officers of the Audit department or nominated authorised staff. For example, Audit and Risk reports which identify security and control weaknesses.		
Preparation and Handling <i>Markings</i> Distinct markings on document or information asset. Centre of top and bottom of each page, in capitals, 5mm (20 point) bold and red if possible. <i>Page Numbering</i> Desirable. <i>Filing:</i> File in distinctive file (blue). Appropriate file cover sheet to be used. <i>Preparation of Electronic Information</i> Prepare in drive or electronic document and records management system with restricted access. <i>SCI Register</i> Desirable. <i>User Auditing</i> Log in/out, failed attempt and Delete. <i>Printing</i> Unless otherwise secured, Printer not to be left unattended.	Removal from workplace, and monitoring <i>Removal of file or document</i> Basis of need. Authorisation of information owner required. Kept in personal custody. Ensure adequate storage arrangements. <i>Monitoring</i> Basic checks only, no need for formal audit.	Copying and storage <i>Copying</i> May be prohibited by information owner. To be kept to a minimum in accord with operational requirements. <i>Physical Storage</i> 'Clear Desk' policy. Lockable cabinet. <i>Electronic Information Storage</i> Restrict logical access based on need-to-know.	
Manual Transmission <i>Within a single location</i> Single opaque envelope indicating classification. Uncovered by hand in discrete office environment. <i>Between locations</i> Single opaque envelope that does not indicate classification. Receipting at discretion of information owner. Delivered by hand or authorised messenger including Australia Post.	Electronic Transmission <i>Data transmission</i> Basis of 'need-to-know'. May be passed unencrypted over appropriately classified internal networks. Information should be encrypted when being sent between agencies. <i>Email</i> Basis of 'need-to-know'. May be passed unencrypted over appropriately classified internal networks. Information should be encrypted (eg via GovNet secure email) when sent between agencies. <i>Fax</i> Required that someone attend the receiving facsimile to receive the material, and that receipt or non-receipt of the document is advised. Encryption is desirable but not mandatory	Archive & Disposal In accordance with authorised retention and disposal schedule issued under Section 26 of the Public Records Act 2002. <i>Paper waste</i> Drafts, working papers and copies may be recycled through lockable classified waste bins. Drafts, working papers and copies may also be shredded. <i>Electronic Media & equipment.</i> Media may be reused or disposed of as per paper waste.	

5.3 PROTECTED

Green folder 	Information whose compromise could cause damage to the State, the Government, commercial entities or members of the public. For instance, compromise could: • endanger individuals and private entities; • work substantially against government finances or economic and commercial interests; • substantially undermine the financial viability of major organisations; • impede the investigation or facilitate the commission of serious crime; or • seriously impede the development or operation of major government policies. As a principle, most non-national security information would be adequately protected by the procedures given to information marked X-IN-CONFIDENCE or PROTECTED. Includes CABINET-IN-CONFIDENCE classified material.	
Preparation and Handling <i>Markings</i> Distinct markings on document or information asset. Centre of top and bottom of each page, in capitals, 5mm (20 point) bold and red if possible. <i>Page Numbering</i> Desirable. <i>Filing</i> File in distinctive file (green). Appropriate file cover sheet to be used. <i>Preparation of Electronic Information</i> Prepare in drive or electronic document and records management system with restricted access. <i>SCI Register</i> Desirable. <i>User Auditing</i> Log in/out, failed attempt, Read, Write and Delete. <i>Printing</i> Printer not to be left unattended while PROTECTED documents are being printed.	Removal from workplace, and monitoring <i>Removal of file or document</i> Basis of need. Authorisation of information owner required. Kept in personal custody. Ensure adequate storage arrangements. <i>Monitoring</i> Regular checks of the Security Classified Information Register and information is desirable. Discussing Classified Information <i>Meetings</i> Must occur behind closed doors in fully enclosed rooms. Notify classification to audience. Material must include classification markings. Remove from equipment and whiteboards prior to vacating room <i>Telephone and video conference</i> Telephone and video conference should not be used for data or voice transmission of material unless both ends are provided with encryption. Cordless or mobile phones should not be used to discuss protected information unless the security they use has been approved by DSD for this classification.	Copying and storage <i>Copying</i> May be prohibited by information owner. To be kept to a minimum in accord with operational requirements. <i>Physical Storage</i> 'Clear Desk' policy. Key lockable steel container (C-Class) in a secure or partially secure environment. Steel-lined, tamper-evident container with a combination lock (B-Class) in an intruder resistant environment. <i>Electronic Information Storage</i> Restrict logical access based on need-to-know.
Manual Transmission <i>Within a single location</i> Single opaque envelope indicating classification. Uncovered by hand directly between authorised members of staff in discrete office environment. Should not be left unattended on recipient's desk. <i>Between locations</i> Double enveloping (i.e. sealed inner envelope indicating classification placed within a single opaque outer envelope that does not indicate classification); or Single opaque envelope that does indicate classification and secured in a lockable container and delivered by an authorised messenger. Receipting required.	Electronic Transmission <i>Data transmission</i> Basis of 'need-to-know'. May be passed over appropriately classified internal networks. Information should be encrypted when being sent between agencies using Transport Layer Security (TLS), Secure Sockets Layer (SSL) or IP Security (IPSec) encryption. <i>eMail</i> Basis of 'need-to-know'. May be passed over appropriately classified internal networks. Information must be encrypted (eg via GovNet secure email) when sent between agencies. <i>Fax</i> Required that someone attend the receiving facsimile to receive the material, and that receipt or non-receipt of the document is advised. Encrypted communications systems must be used to transmit PROTECTED information.	Archive & Disposal In accordance with authorised retention and disposal schedule issued under Section 26 of the Public Records Act 2002. <i>Paper waste</i> Drafts, working papers and copies must be shredded. <i>Electronic Media & equipment</i> Media to be destroyed or sanitised.

5.4 HIGHLY PROTECTED

Salmon pink folder 	Information that requires a substantial degree of protection as compromise of the information could cause serious damage to the State, the Government, commercial entities or members of the public. For instance, compromise could: • threaten life directly; • seriously prejudice public order; or • substantially damage government finances or economic and commercial interests. Very little information belongs in the HIGHLY PROTECTED category and the marking should be used sparingly. Note: A common representation of Salmon Pink in the RGB colour space is 250, 128, 114.		
Preparation and Handling <i>Markings</i> Distinct markings on document or information asset. Centre of top and bottom of each page, in capitals, 5mm (20 point) bold and red if possible. <i>Page Numbering</i> Essential. Numbering should be of the form 'Page n of x' where x is the total number of pages. Copies should be numbered. <i>Filing</i> Must be placed in appropriate file without delay. File in distinctive file (salmon pink). Use file reference and folio numbering. Appropriate file cover sheet to be used. <i>Electronic Information</i> Prepare in drive or electronic document and records management system with restricted access or on standalone equipment. <i>SCI Register</i> Register essential. Additionally requires information on all copies, as per section 3.6 of the QGISCF. <i>User Auditing</i> Log in/out, failed attempt, Read, Write, Modify and Delete. <i>Printing</i> Printer not to be left unattended while HIGHLY PROTECTED documents are being printed.	Removal from workplace, and monitoring <i>Removal of file or document</i> Basis of need. Authorisation of information owner required. Kept in personal custody. Ensure adequate storage arrangements. Must maintain a record of removal (i.e. via Security Classified Information Register). <i>Monitoring</i> Regular checks of the Security Classified Information Register and information is essential.	Copying, storage and disposal <i>Copying</i> May be prohibited by information owner. To be kept to a minimum in accord with operational requirements. Copies should be numbered. <i>Physical Storage</i> 'Clear Desk' policy. Steel-lined, tamper-evident container with a combination lock (B-Class) in a partially secure environment, or key lockable steel container (C-Class) in a secure environment. Steel-lined, concrete strengthened container with a combination lock (A-Class) in an intruder resistant environment. <i>Electronic Information Storage</i> Restrict logical access based on need-to-know.	
Manual Transmission <i>Within a single location</i> Single opaque envelope indicating classification. Uncovered by hand directly between authorised members of staff in discrete office environment. Should not be left unattended on recipient's desk. <i>Between locations</i> Double enveloping (i.e. sealed inner envelope indicating classification placed within a single opaque outer envelope that does not indicate classification); or Single opaque envelope that does indicate classification and secured in a lockable container and delivered by an authorised messenger. Receipting required.	Electronic Transmission <i>Data transmission</i> Basis of 'need-to-know'. May be passed over appropriately classified internal networks. Information must be encrypted when being sent between agencies using Transport Layer Security (TLS), Secure Sockets Layer (SSL) or IP Security (IPSec) encryption. <i>eMail</i> Basis of 'need-to-know'. Email should be the last resort for the distribution of HIGHLY PROTECTED documents unless the document is separately encrypted to an appropriate standard. Email is to contain the classification in the 'Subject' line. The 'Prevent copying' option in the 'Delivery Options' is to be checked. May be passed unencrypted over appropriately classified internal networks. Information must be encrypted (eg via GovNet secure email) when being sent between agencies. <i>Fax</i> Required that someone attend the receiving facsimile to receive the material, and that receipt or non-receipt of the document is advised. Encrypted communications systems must be used to discuss or transmit HIGHLY PROTECTED information.	Archive & Disposal In accordance with authorised retention and disposal schedule issued under Section 26 of the Public Records Act 2002. <i>Paper waste</i> Drafts, working papers and copies must be shredded. <i>Electronic Media & equipment</i> Media to be destroyed or sanitised.	

6 Non-General Control Details

6.1 Discussing security classified information

All discussions of HIGHLY PROTECTED or PROTECTED information should occur behind closed doors in fully enclosed rooms. If discussions of X-IN-CONFIDENCE information are held, care should be taken to ensure that people without a need to know are not able to overhear the discussions.

When it is necessary to discuss security classified information in meetings (including in-person meetings, presentations, teleconferences, and video conferences), convenors should take appropriate steps to ensure that the audience is restricted to those with a need-to-know and that the risk of compromise of security classified information is minimised by ensuring seating arrangements preclude the possibility of information be viewed without proper authority.

Where meetings are held, the security classification of the information should be notified to the audience and the audience reminded of their responsibility to maintain confidentiality.

Visual aids such as slides and overhead transparencies should include the appropriate security classification markings and should be removed at the conclusion of the meeting, including deleting the presentation from corporate resources such as laptops.

Any security classified information placed on whiteboards should be erased with a suitable cleaner prior to the room being vacated.

6.1.1 Telephone and video conference

An agency's private video conference, telephone or intercom systems using wireline or fiberoptic transmission paths only (that is, no microwaves or similar radio frequency links) may be used to pass voice or facsimile information classified X-IN-CONFIDENCE without further precautions. For PROTECTED and HIGHLY PROTECTED information, additional encryption, or the use of approved secure communications systems, is required.

Mobile telephones should not be used for data or voice transmission of security classified information unless both handsets are provided with encryption appropriate to the classification of information being transmitted.

6.1.2 Records of discussion and/or presentation

Agencies will exercise discretion in regard to this aspect of information security. Where an agency decides it is applicable, a record should be taken of all discussions and presentations of HIGHLY PROTECTED and PROTECTED information. The record should detail the:

- nature of the material presented;
- date;
- audience present;
- decisions made; and
- actions to be taken.

All records taken during the presentation or discussion of security classified information should assume the same security classification.

6.2 Copying security classified information

Classified information should only to be reproduced when it is strictly necessary to do so. Spare or spoilt copies of security classified information should be destroyed immediately in accord with the appropriate disposal requirements.

When making copies of information that has a copy number (especially PROTECTED and HIGHLY PROTECTED material), the permission of the information owner must be obtained. When seeking permission to make copies, the proposed additional distribution should be provided and the owner should indicate the appropriate copy numbers.

Copiers should not be left unattended if classified information is being reproduced unless there are suitable physical access controls to prevent unauthorised persons (including those without a need-to-know) from both entering the area around the copier, and viewing the material being printed.

6.3 Storage of security classified information and associated media

The following section applies equally to the storage of physical information (paper etc) and electronic information. Electronic storage media¹⁵ (discs, CD Towers etc) containing classified information must be afforded the full protection given to equivalent classified hard copy information. Due to the risk of accidental loss and lack of movement control and audit trails, classified information stored on stand-alone or portable computers, hard drives, flash memory drives, and other storage devices must be treated with the same controls applicable to removable media including the use of encryption and storage where applicable in secure containers.

Where possible, this type of media must be clearly labelled in accordance with the security classification level of the data stored on the media, unless the classified information has been encrypted in accordance with ACSI-33, Part 3, Chapter 9 or a similar approved agency cryptography framework. If encryption systems do not encrypt the entire media content, care must be taken to ensure that either all of the classified data is encrypted appropriately or that the media is handled in accordance with the highest classification of the unencrypted data.

Electronic storage media includes fixed or removable storage and can be either

- volatile storage, which loses its information when power is removed, or
- non-volatile, which retains its information when power is removed.

Volatile media used to process classified material may be treated as UNCLASSIFIED once the power has been removed. As noted previously, any non-volatile media containing classified material should be labelled appropriately. In the case of internally mounted hard-drives, the computer case should be labelled.

Suitable storage for classified material and electronic media should be determined by a risk assessment. The type of secure storage device or area required is dependant upon a number of factors including:

- the classification of the information asset;

¹⁵ In the context of this framework, media is the component of computer hardware that is used to store information.

- the type of information access facility where the information is located;
- the value and attractiveness of the information to be stored;
- the structure and location of the building;
- entry control systems; and
- other physical protection systems (for example, locks and alarms).

Depending on the outcomes of the risk assessment and taking into account the various factors mentioned above, secure storage may range from (but is not limited to) lockable drawers, secure filing cabinets or compactus, to secure rooms. The following table sets out the recommended minimum standard of security container that can be used for a type of secure room¹⁶.

Security Classification	Secure Areas	Partially Secure Areas	Intruder Resistant Area
Highly Protected	C-class container	B-class container	A-class container
Protected	C-class container	C-class container	B-class container
X-In-Confidence	Agency discretion	Lockable cabinet	Lockable cabinet

Table 6- Recommended minimum standard of security container

The following table describes the minimum requirements of secure containers.

Class	Features
A	Steel-lined, concrete-strengthened container secured with an appropriate combination lock
B	Steel-lined, tamper evident container with an appropriate combination lock
C	Key lockable, steel container

Table 7- Minimum Requirements of security containers

Secure, Partially Secure or Intruder Resistant Areas are areas that have measures in place for the secure handling and storage of security classified information. They may be a single room, a building, or a complex consisting of a number of buildings.

The descriptions about what constitutes a Secure, Partially Secure, and Intruder Resistant Area are provided in the following Table. These descriptions have been adapted from the *Protective Security Manual* to assist the organisation when selecting appropriate handling and storage measures, including suitable containers.

¹⁶ The Commonwealth Government specifies appropriate containers in its Security Equipment Catalogue (SEC) which is managed by the Australian Security Intelligence Organisation (ASIO).

Control Measure	Secure Areas	Partially Secure Areas	Intruder Resistant Area
tamper-evident barriers, highly resistant to covert entry ¹⁷	Yes	Yes	Yes
an effective means of providing access control during both operational and non-operational hours	Yes	Yes	Yes
all persons to wear passes	Yes	Yes	Yes
all visitors escorted at all times	Yes	Yes	Yes
appropriately secured points of entry and other openings	Yes	Yes	No
during non-operational hours a monitored security alarm system, providing coverage for all areas where security classified information is stored	Yes	Yes	No
an approved means of limiting entry to authorised persons	Yes	No	No

Table 8- Description of security areas

The standard and combination of the measures should be in keeping with the highest level of security classified information protected in the area. The measures must ensure that the less effort and time required to gain access to the information, the quicker the detection and response must be to the security incident. Conversely, the better the physical security barriers protecting the information, the greater the time can be allowed for the detection and response to the security incident.

6.4 Electronic authentication and access controls

In addition to physical access controls, agencies must have a means of controlling access to their computer systems or networks. All computer-resident classified information should have authentication and access controls to ensure that only authorised users can access the information and it is not improperly disclosed, modified, deleted, or rendered unavailable. In addition, the computer and communications system privileges of all users, systems and programs should be restricted on a need-to-know basis. Authentication controls must be based on those documented within the *Queensland Government Authentication Framework*, which provides considerable additional detail concerning appropriate authentication controls and mechanisms.

When implementing controls to restrict logical access to certain resources, agencies should:

- Limit user access on the basis of Need-to-know,
- Provide users with the minimum of privileges required for their job, and
- Require requests for access to a system be authorised by the information owner or other approval authority.

¹⁷ Such barriers provide containment in all directions. They have enough resistance to covert entry to provide some assurance that a person attempting to gain unauthorised entry and exit without being apprehended would have to damage or modify the barriers so that it was obvious that a security incident had occurred.

To ensure that access and back-up of electronic information remain tightly controlled and monitored, classified information in electronic form is best stored and managed through an electronic document and records management system (eDRMS) or other system with appropriate equivalent functionality.

At a minimum, information kept on network file-servers must be kept in locked files designated for defined user groups and individual users.

6.5 Audit logs

To maintain confidentiality and integrity of classified information a strict audit logging process is to be implemented, with traceability provided from the security classified information register. This audit log must be carefully designed to ensure it is capable of providing a “trail of evidence” which can be used to investigate inappropriate or illegal access.

Care must be taken that the audit log therefore logs all information which is useful in constructing this trail of evidence. Audit log access controls must be in place with explicit user authentication (also logged) needed to view the audit log database. The levels of auditing required for security-classified information are shown in Table 9.

Audit Log Controls		
Information Security Classification	General User / Files	Administrator
HIGHLY PROTECTED	Log In/Out, Failed Attempts, Read, Write, Modify & Delete	Log In/Out, File Access. Administrators are not to have Read, Write, Modify or Delete access to audit logs
PROTECTED	Log In/Out, Failed Attempts, Read, Write & Delete	Log In/Out, File Access. Administrators are not to have Read, Write, Modify or Delete access to audit logs
IN-CONFIDENCE	Log In/Out, Failed Attempts & Delete	Log In/Out, File Access. Administrators are not to have Read, Write, Modify or Delete access to audit logs
Unclassified	Log In/Out, Failed Attempts,	Log In/Out, File Access. Administrators are not to have Read, Write, Modify or Delete access to audit logs

Table 9- Levels of auditing required for classified information

6.6 Email transmission

Internal networks can be used to transmit in-confidence or higher classified data (although email should be a last resort for HIGHLY PROTECTED assets). When internal networks are used to transmit classified information, care must be taken to ensure that all mail servers involved in the transaction are appropriately secured to the required security classification.

If in-confidence or higher data is passed between agencies without using the GovNet secure mail service it must be encrypted to an appropriate level. However, email should be the last resort for transmission of highly protected assets.

6.7 Facsimile transmission

All staff must have awareness of transmission of information using facsimile in line with the need-to-know guidelines in this document. When transmitting any security classified material it is a requirement that someone attend the receiving facsimile to receive the material, and that receipt or non-receipt of the document is advised. For PROTECTED and HIGHLY PROTECTED there is an additional requirement that the link is encrypted. These controls are detailed in the following table.

Measure	UN-CLASSIFIED	IN-CONFIDENCE	PROTECTED	HIGHLY PROTECTED
Requires encrypted link	No	No	Yes	Yes
May be faxed internally and externally if the recipient is standing by the receiving fax machine and there is no opportunity for any unauthorised person to view the document.	Not Applicable	Yes	Yes	Yes
Receiving officer is to acknowledge receipt or non-receipt of the document within 10 minutes of its transmission	No	Yes	Yes	Yes

Table 10- Facsimile transmission measures

7 References

7.1 Queensland Government legislation

Financial Administration and Audit Act 1977

<http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/F/FinAdminAudA77.pdf>

The *Financial Administration and Audit Act 1977* sets out the principles to be observed by agencies in relation to their financial management and audit practices. Section 36 of the Act describes the responsibilities of the accountable officer (usually the Director-General) which include establishing and maintaining suitable systems of internal control and risk management, and complying with the financial management standards.

Financial Management Standard 1997

<http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/F/FinAdminAudSt97.pdf>

The *Financial Management Standard 1997* provides detailed governance policy to be observed by all public sector agencies including financial management, internal controls, risk management strategies, operational planning, user charging, resource management and annual reports. In particular, Sections 22 (2) and 56 (2) articulate the requirement to comply with the mandatory principles of the Queensland Government Information Standards.

Public Records Act 2002

<http://www.legislation.qld.gov.au/LEGISLTN/ACTS/2002/02AC011.pdf>

Public Records Act 2002: A Plain English Guide, Queensland State Archives

(<http://www.archives.qld.gov.au/downloads/PRAplainenglishguide.pdf>)

Public Sector Ethics Act 1994

<http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/P/PublicSecEthA94.pdf>

7.2 Queensland Government standards

Queensland Government Cabinet Handbook

http://www.premiers.qld.gov.au/About_the_department/publications/policies/Governing_Queensland/Cabinet_Handbook/

Queensland State Archives (2004) Management of ASIO documents in Queensland Public Records

<http://www.archives.qld.gov.au/downloads/ASIOGuidelines%20.pdf>

All current Queensland Government Information Standards are available from

http://www.governmentict.qld.gov.au/02_infostand/standards.htm

Of particular relevance to this framework are:

Information Standard 2 - ICT Resource Planning

Information Standard 18 – Information Security

Information Standard 18 – Information Security Best Practice Guide

Information Standard 31 - Retention & Disposal of Public Records (IS31)

Information Risk Management Best Practice Guide

Information Standard 40 – Recordkeeping

Information Standard 42 – Information Privacy (IS42)

Information Standard 42A - Information Privacy for the Queensland Department of Health (IS42A)

7.3 Australian Government standards

Protective Security Manual 2005, Australian Government, Attorney General's Department, 2005. (Restricted distribution, available by request)

http://www.ag.gov.au/agd/WWW/protectivesecurityhome.nsf/Page/Protective_Security_Manual

The *Protective Security Manual* (PSM) sets out the policies, practices and procedures that Australian Government agencies use to protect the agency and its assets. Whilst this guide adopts a similar set of controls to the PSM and associated guidance, including the Australian Government Information Technology Security Manual (ACSI 33), these controls have been tailored, and compliance with this guide would not infer compliance with Australian Government requirements.

Australian Government Information Technology Security Manual (ACSI 33) – Defence Signals Directorate

http://www.dsd.gov.au/lib/pdf/doc/acsi33/acsi33_u.pdf

Australian Government Electronic Authentication Framework: An Overview for Australian Businesses, AGIMO, June 2004.

<http://www.agimo.gov.au/infrastructure/authentication>

7.4 Australian standards

Australian Standards are available for purchase from SAI Global.

<http://www.saiglobal.com/shop/Script/search.asp>

AS/NZS ISO/IEC 17799:2001: Information technology – Code of practice for information security management

AS/NZS 7799.2:2003: Information security management - Specification for information security management systems

AS/NZS 4360:2004: Risk Management

8 Glossary

Term	Definition
SCIR - Security Classified Information Register	A register, electronic or paper database that provides a record to keep track of security classified information asset attributes.
Critical Information Assets	Information Assets key to the core operation, performance, capability, viability and credibility of the agency.
Declassification of media	Declassification is an administrative decision to remove all classifications from the media, based on an assessment of relevant issues including the consequences of damage from disclosure or misuse, the effectiveness of any sanitisation procedure used, and the intended destination of the media.
Information Assets	Information assets are information in any form including but not limited to documents, files, images, samples, and electronic data.
Information Asset Security Domain	An information asset security domain is a grouping of related information assets that share a security classification. Security domains allow a defined level of security classification to be automatically assigned to assets of the domain. This helps to ensure consistency and reduce owner and user/editor workloads. See section 2.5 for more information.
Information Owner	The recognised officer who is identified as having the authority and accountability for one or more information assets. See Section 2.6.1 for a full definition.
Reclassification of media	Reclassification is an administrative decision to change the classification of media, based on an assessment of relevant issues including the consequences of damage from unauthorised disclosure or misuse, the effectiveness of any sanitisation procedure used, and the intended destination of the media.
Security Controls	Hardware, programs, procedures, policies and physical safeguards which are put in place to assure the integrity and protection of information and the means of processing and accessing it.
User/Editor	Staff that use, edit or originate information assets. See Section 2.6.2 for a full definition.

- End of Queensland Government Information Security Classification Framework -