Information Management Advice 33 Implementing Information Security Classification

Part 2: The Security Classification Process

Introduction

This Advice outlines issues to consider when implementing the Tasmanian Government Information Security Classification Framework. It is intended for use by information management professionals within agencies to assist them in establishing effective security classification practices.

Approach

Agencies will need to determine the extent to which security classification needs to be applied to information assets. The security classification of information assets should meet both business and operational needs. It should be based on a risk assessment and business impact analysis.

This Advice can be used by all agencies to evaluate the security classification of their information assets. Ideally, classification labels 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 Advice 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 considered appropriate, agencies will likely find it helpful to develop their own set of impact considerations with examples pertinent to agency business. This will help ensure staff have relevant and understandable guidance, resulting in better security classification decisions.

It is recognised that the implementation of security classification will be progressive in nature. It is therefore recommended that security classification be applied in the following order:

1. All new information assets should be evaluated against Information Security Classification (ISC) during their acquisition or creation.
2. All information assets involved in existing information transfers, either outgoing from the agency or incoming.
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).

5. The remaining existing information assets should be evaluated against ISC based on an assessment of risk, with high risk information assets being considered a priority for evaluation.

The Security Classification Scheme

This section outlines the schema to be used for security classification of information assets within the Tasmanian Government. Information assets are valuable government resources, and as such they:

- 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
- must only be released in accordance with the policies, legislative requirements and directives of the Government and the courts.

Information assets typically fall into two broad categories:

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

Figure 1 below provides a representation of the various security classifications of official Government information.

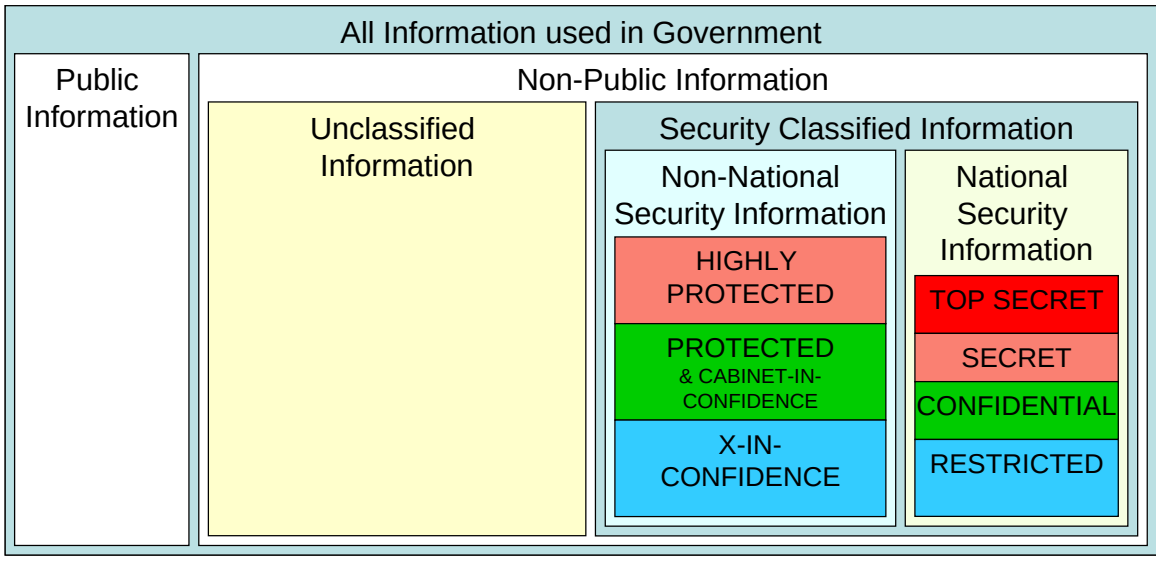

Figure 1: Government information security classifications

Public Information is information authorised for unlimited public access such as agency websites. The integrity of public domain information must be ensured before its release. Examples include publications and annual reports.

Unclassified information must be accessed and used observing the need-to-know principle and afforded a level of security to protect confidentiality. Unclassified information is information that is not in the public domain, but does not need to be classified. Examples include procedure manuals, departmental memos to general staff and policy documents.

National Security Information is classified based on the Commonwealth Protective Security Policy Framework (PSPF). Agencies need to identify which business units within the agency received national security classified information and ensure it is handled correctly according to its national security classification.

TAHO
Tasmanian Archive + Heritage Office

Example of Information Security Classification

Classification	Description	Examples of Information Assets	Examples of Risk Impacts
PUBLIC	Information that has been authorised by the owner/custodian for public access and circulation. It is important that agencies maintain the integrity and availability of PUBLIC information. Until public access is authorised, it is common for information to have some access restrictions applied by using a non-public security classification. No assurance regarding the identity of individuals accessing PUBLIC information is required. Compromise could cause loss of confidence in the Government and limited damage to commercial entities or members of the public. PUBLIC does not mean that information will be supplied to the general public free-of-charge in all cases. UNCLASSIFIED information may need 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 into the public domain. As a minimum, UNCLASSIFIED information requires only minimal confidence in the identity of the individual accessing the information (Access Assurance Level 1).	Publications Public Register Jobs postings - jobs.tas.gov.au	Insignificant or Minor Little or no degradation of the capacity (i.e. efficiency or effectiveness) of the agency to perform one or more of its functions Little or no impact on individuals through some minor injuries may be present Minor financial impact to agency of between 2% and 5% of the monthly agency budget or impact to individuals of up to $2000 Little or no impact on community confidence in the agency ability to deliver essential services Minimal inconvenience if not available. If lost, changed or denied would not result in injury to an individual or government (that is, no legal effect)
UNCLASSIFIED	UNCLASSIFIED information may need 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 into the public domain.	Ordinary staff meeting agendas and minutes Research and background papers (with no copyright	Insignificant or Minor Little or no degradation of the capacity (i.e. efficiency or effectiveness) of the agency to perform one or more of its functions

Classification	Description	Examples of Information Assets	Examples of Risk Impacts
	As a minimum, UNCLASSIFIED information requires only minimal confidence in the identity of the individual accessing the information (Access Assurance Level 1).	restrictions) procedure manuals departmental memos to general staff policy documents	Little or no impact on individuals through some minor injuries may be present Minor financial impact to agency of between 2% and 5% of the monthly agency budget or impact to individuals of up to $2000 Little or no impact on community confidence in the agency ability to deliver essential services Minimal inconvenience if not available. If lost, changed or denied would not result in injury to an individual or government (that is, no legal effect)
X-IN-CONFIDENCE	Information that if compromised could cause limited damage to the State, the Government, commercial entities or members of the public. As a minimum, requires a low level of confidence in the identity of the individual accessing the information (Access Assurance Level 2). Compromise could: cause distress to individuals or private entities; cause financial loss or loss of earning potential, or facilitate improper gain or advantage; 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; and/or undermine the proper management of the public sector and its operations. This protective marking includes a notification of the subject matter (X), which alludes to its audience and the need-to-know principle (this does not include CABINET-IN-CONFIDENCE, see	Personal case files such as entitlements, program files or personnel files Industrial trade secrets Registration information Policy Advice Policy interpretation Draft request for proposals 3rd party business information submitted in confidence Tender evaluations Complaints	Loss of operational systems or reduced ability for the agency to perform one or more of its functions lasting between 1 to 7 days Inability of the agency to perform one or more if its functions where top level management or ministerial intervention would be required Low to series levels of injuries or illness to individuals Significant to major financial impact to the agency between 5% and 10% of the monthly agency budget or impost to individuals of between $2000-$20,000 Community confidence lowered in the agency ability to perform one or more of its functions where a measure of damage control may be required High degree of risk if corrupted or modified Disruption to business if not available

Classification	Description	Examples of Information Assets	Examples of Risk Impacts
	PROTECTED). Examples include: STAFF-IN-CONFIDENCE: includes all official staff records where access would be restricted to HR personnel and nominated authorised staff. For example, personnel 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 or other commercial information such as sensitive intellectual property. For example, draft requests for offer information, tender responses, tender evaluation records, designs and government research.		
PROTECTED	Information that if compromised could cause damage to the State, the Government, commercial entities or members of the public. As a minimum, requires a moderate level of confidence in the identity of the individual accessing the information (Access Assurance Level 3). 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, and/or seriously impede the development or operation of major government policies. Generally, most non-national security information would be adequately protected by the procedures given to information marked X-IN-CONFIDENCE or PROTECTED.	Cabinet Documents Cabinet deliberations and supporting documents Personal medical records Criminal records Criminal Investigations	Loss of operational systems or reduced ability for the agency to perform one or more of its functions lasting between 1 to 7 days Inability of the agency to perform one or more if its functions where top level management or ministerial intervention would be required Low to series levels of injuries or illness to individuals Significant to major financial impact to the agency between 5% and 10% of the monthly agency budget or impost to individuals of between $2000-$20,000 Community confidence lowered in the agency ability to perform one or more of its functions where a measure of damage control may be required High degree of risk if corrupted or modified

Classification	Description	Examples of Information Assets	Examples of Risk Impacts
	Includes Cabinet submissions and decisions to be marked CABINET-IN-CONFIDENCE.		Disruption to business if not available
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. As a minimum, requires a high level of confidence in the identity of the individual accessing the information (Access Assurance Level 4). For instance, compromise could: threaten life directly, seriously prejudice public order, and/or substantially damage government finances or economic and commercial interests. Generally, very little information belongs in the HIGHLY PROTECTED category.	Budget prior to public release	Inability to operate and deliver essential agency operational functions and services where the delivery is significantly compromised for a significant time period for greater than 7 days Major loss of life and serious levels of life threatening injuries or illness to many individuals Major financial impost to the agency in excess of 10% of the monthly agency budget or agency impost to individuals of in excess of $20,000 Extreme publicity causing embarrassment to the agency or government resulting in a seriously loss of public confidence Compromise of Cabinet deliberations Destructions of partnerships and relationships Sabotage/Terrorism Extreme risk if corrupted or modified

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' 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.

An example of an existing domain classification is cabinet documents, which are pre-determined as being CABINET-IN-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.

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

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 classifications need 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 in Figure 1 (below) is expanded in more detail in the following sub-sections.

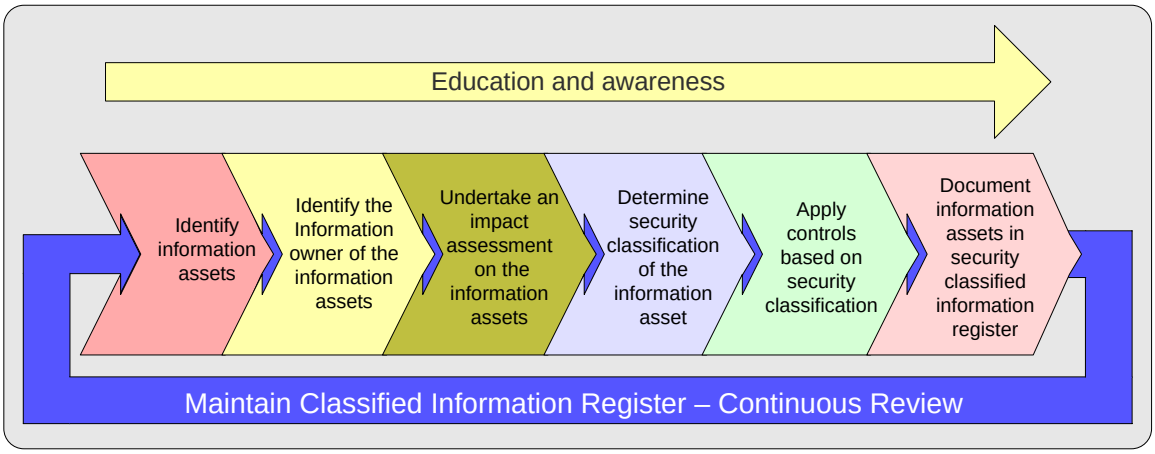

Figure 1: Information Security Classification Process

Step1 : Identify Information Assets

Information assets are defined as an identifiable collection of data, stored in any manner and recognised as having value for the purpose of enabling an agency to perform its business functions, thereby satisfying a recognised agency requirement.

Examples of information assets include, but are not limited to:

- records
- documents
- electronic messages
- rows in a database
- tables or figures within a document
- whole database tables
- collections of data objects about a single logical entity or concept such as 'customer'
- content identified through - Uniform Resource Locators (URLs) or Uniform Resource Identifiers (URIs)
- metadata about other information assets.

Information spanning multiple media types or formats must ensure classification requirements are applied to all types or formats, 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 ISC, but will require additional agency policies to ensure consistent evaluation and application.

'Information asset' is not used to refer to the technology used to store, process, access and manipulate information, which are more properly described as Information and Communication Technology (ICT) assets. ICT assets which are *not* considered information assets include:

- software including application and system software, development tools and utilities, and the associated licences

- 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.

ICT assets should be secured based on the security classification of the information assets they store, use or transmit.

For more Advice on developing an Information Asset Register see *Advice 39 Developing an Information Asset Register*.

Step 2: Identify the owner of the Information Assets

Each agency is responsible for ensuring that information assets have a security classification that is authorised by the information owner, and that a custodian who is responsible for implementing and maintaining information assets, according to the rules set by the owner, has been assigned. Information assets 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 assets that are externally generated, and not otherwise classified, the agency officer who receives them should ensure that an owner and custodian are assigned, and that the asset is incorporated into agency information asset registers as appropriate.

See *Advice 40 The Role of an Information Asset Owner* and *Advice 38 Information Asset Owner and Digital Continuity* for more detail on information asset ownership and custodianship.

Step 3: Impact assessment of information assets for the Risk Analysis

The purpose of the assessment is to identify what the probability or likelihood of the threat is and what the impact would be if there was a loss to the integrity, availability, confidentiality or the value of information assets. Risk assessments are undertaken to properly identify risks.

When determining the correct information security classification level for an information asset or domain, a range of considerations need to be taken into account. Where information assets 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 assets where 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 (e.g.

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 an information asset may affect its security classification, and therefore 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 assets that are 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 asset to be published and made available to the public.

IMPACT Type	**Severity** Lowest → Highest				
Impact Severity	**None/ Negligible**	**Minor**	**Moderate**	**Major**	**Severe**
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	None/Negligible		Measurable Impact	Prejudice	Seriously prejudice
Inappropriate release of personally or commercially sensitive data to third parties	No or Negligible release of sensitive information	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[1] of the service provider or third party	No or Negligible Loss	Minor loss	Moderate loss	Significant loss	Substantial loss
Financial Loss to Agency / Service Provider	No or Negligible Loss	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[2]	No or Negligible threat			Agency business or service delivery impaired in any way	Agency business halted or significantly impaired for a

[1] In order to assist in the determination of the appropriate level of impact, the following is suggested: Minor <$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.

[2] 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.

IMPACT Type	Severity Lowest				Highest
					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
Impact on the environment	None/Negligible	Minor impact on the environment.	Measurable short term damage to the environment	Limited long term damage to the environment	Substantial long term damage to the environment
Impact on agency or Tasmanian Government workforce	None/ Negligible	Minor impact	Measurable impact	Limited long term impact	Substantial long term impact
Impact on risk of litigation	None/ Negligible	Minor impact	Measurable impact	Significant impact	Substantial impact
	⇩	⇩	⇩	⇩	⇩
SECURITY CLASSIFICATION	**Consider for PUBLIC or UNCLASSIFIED**	**UN-CLASSIFIED**	**X-IN- CONFIDENCE**	**PROTECTED**	**HIGHLY PROTECTED**

Table 1: Impact assessment matrix
Example sourced from the Queensland Government Information Security Framework

To provide some assistance in completing the impact assessments, Table 2 below 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. Examples could include release of names or locations of under-cover officers, people under protection orders.
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. For example, if inappropriate access to information was granted, 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.

Impact type	Possible considerations
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).
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).
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 2: Impact considerations sourced from the Queensland Government Information Security Framework

Step 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. Table 3 below outlines the analysis of a particular information asset impact assessment: In this example, the highest impact identified is major, and hence should be classified as PROTECTED.

As mentioned earlier, other agency, regulatory or legislative issues including those arising from the *Archives Act 1983* also impact on the security classification of the information, and need to be considered at this point.

Consequence	**Impact Severity**
Risk to Individual safety	None
Distress caused to any party	Major
Damage to any party's standing or reputation	Major
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[3] 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 3: Example impact assessment from the Queensland Government Information Security Framework

[3] 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.

Application specific considerations

There are two common agency ICT applications that need specific considerations when identifying information assets, namely, Electronic Document and Records Management Systems (EDRMS) and web content management systems.

EDRMS

When considering classifying an EDRMS as an information asset, it is tempting to identify information assets that relate to the content of the documents and records held within the system. This is especially true when the EDRMS holds complete electronic copies of the source documents.

However, for the purpose of ISC, an EDRMS is considered to contain information about the tracking of files and documents. The contents of any documents or files it holds are to be dealt with separately. If this limitation is not applied, an EDRMS could potentially map to the majority of domains within the classification framework. Such a scenario would provide little value for future analysis.

A more valuable approach is to identify an EDRMS as containing information assets such as business records repository or file and records inventory (or similar names according to each agency's terminology). It is then recommended that agencies apply a classification to the whole system.

The situation with an EDRMS may also manifest in other similar pure catalogue, tracking or inventory systems, such as library cataloguing.

Static website content and web content management systems

As with EDRMS, agency websites and associated web content management systems (WCMS) pose their own unique challenges for information asset identification, and subsequent classification.

For the purpose of ISC it is recommended that static website content is broken down into information assets that match the site (navigation) structure (or division of information within the web content management system). Each of these main areas, once treated as an asset, can then be classified. When classifying information assets based on web content, it is suggested that agencies apply classification at the domain level.

If a website contains a dynamic application or is the gateway for an application then the dynamic component or application may generate its own set of information assets.

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. For example 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 asset may decrease over time, for example budget documents that may be 'BUDGET-IN-CONFIDENCE (until tabled on 15 Jun 13)'. Some information assets may require increased protection because it is under embargo until a specific public policy statement, 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 asset- 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 Right to Information purposes.

Step 5: Apply Controls Based on Security Classification

Appropriate controls must be applied to ensure that protection is given to information assets commensurate with the security classification level that has been determined. These controls are outlined in section Part 3 of this Advice.

Step 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 information assets. HIGHLY PROTECTED and PROTECTED information assets must be captured in a SCIR; it is also highly desirable for X-IN-CONFIDENCE assets to be captured. The security classified information register may be a sub-set of an overall agency information asset register, and may be established using existing asset control or document and records management systems.

The SCIR will ideally be 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. As a minimum, the SCIR should include:

- name or unique identifier of asset or group of assets (e.g. a unique file number or name, data base name)
- description of information asset (ie. what is it about)
- location of information asset, including the device on which it is stored
- information owner/custodian
- security classification of the information asset
- date of security classification commences with details of the authority of the classifier (eg who approved the classification)

IT could also include the following:

- 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)
- date to review security classification (if known).
- users and usage of the information
- number of copies in circulation and their location
- 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 assets they manage, and *may* be capable of automatically populating and maintaining a security classified information register for the information assets they control.

The SCIR is, in itself, an information asset, and, with due care as to the information recorded in it, such an inventory of information assets would should have a default classification of SECURITY-IN-CONFIDENCE because of the detail it provides on other security classified information. Agencies should make their own assessment of the security classification of the SCIR and 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 PROTECED information assets to ensure that these are accounted for and are being handled, stored, etc, in accordance with the minimum standards set out in the manual. It is good security practice to conduct a similar spot check of other security classified information assets at irregular intervals.

The SCIR itself should be reviewed and maintained at least annually to ensure it meets the requirements of the ISC and agency needs.

Ongoing Activities

Document the capabilities of technology and application systems

To facilitate application of appropriate controls to information security classified information, agencies should consider documenting the capability of their applications and systems to support the different information security classification levels.

By exploring and documenting the capabilities of their applications and technologies, agencies can reduce the risk that security classified information assets will be mishandled. In turn, this can form part of ongoing education and awareness activities to ensure staff are empowered to handle security classified information assets correctly.

Where security classified information assets will be passed via a number of different applications or technologies, only the lowest security classification within the chain can be assured.

The capability of applications and systems to support different information security classification levels should be reviewed periodically, and when upgrades occur, to ensure controls are maintained.

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. Agencies should ensure that all employees have a clear understanding of the agency information security classification policies and procedures, their responsibilities, and the NEED-TO-KNOW principle. Employees who create, process or handle security classified information assets should be trained in how to handle classified information.

Education and awareness programs will likely vary across an agency, and between agencies, and depend on the type of work and types of information assets 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 other classification levels.

Maintain Security Classified Information Register – continuous review and de-classification

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

Security classification makes information assets more expensive to handle, store and transfer, so it is important to ensure the information security classification is appropriate. This may require de-classifying information assets that are no longer sensitive, or increasing the classification where the consequence of compromise has changed. Information owners should use the SCIR to annually review information asset security classifications.

Declassification

Information assets must be declassified or downgraded when protection is no longer required, or is no longer required at the original level. If a user 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.

Ideally, information asset declassification triggers will be set when the initial classification is applied, and should be captured in the SCIR. Declassification triggers may include:

- a set time period after the creation of an information asset (i.e. 2 years after creation)
- a set period after the last action on an asset (i.e. 6 months after last use)
- passing of a set date (e.g. to be reviewed in January 2020)
- after circumstances that have a direct impact on the asset change significantly (such as a change of strategic priorities or a change of government).

Further Advice

For more detailed advice, please contact:

Government Information Strategy Unit
Tasmanian Archive and Heritage Office
91 Murray Street
HOBART TASMANIA 7000
Telephone: 03 6165 5581
Email: gisu@education.tas.gov.au

Acknowledgements

- Queensland Government Information Security Classification Framework, ICT Policy and Coordination Office, Department of Public Works
- Information Security Classification Government of Alberta

Information Security Classification

This document has been security classified using the Tasmanian Government Information Security classification standard as PUBLIC and will be managed according to the requirements of the Tasmanian Government Information Security Policy.

Document Development History
Build Status

Version	Date	Author	Reason	Sections
2.0	March 2015	Christine Woods	Template	All
1.0	March 2014	Allegra Huxtable	Initial Release	All

Amendments in this Release

Section Title	Section Number	Amendment Summary
All	All	Document imported into new template

Issued: March 2014

Ross Latham
State Archivist