Please do not quote

Information Classification Policy
for
Government Organizations

Information and Communication Technology Agency of Sri Lanka

Table of Contents

1 Introduction 2
1.1 Impact Levels related to Information Assets of an Organization 2
2 Information Classification 5
2.1 Assigning Information Classification 6
2.2 Altering Information Classification 6
2.3 Duration of the Security Classification 6
2.4 Levels of Security Classification 7
2.4.1 Unclassified 7
2.4.2 Public 8
2.4.3 Limited Sharing 8
2.4.4 Confidential 9
2.4.5 Secret 9
3 The Information Classification Process 10
3.1 Step1: Identify Information Assets 10
3.2 Step 2: Identify the owner of the Information Assets 11
3.3 Step 3: Impact assessment of information assets for the Risk Analysis 12
3.4 Step 4: Determine the Security Classification of the Information Asset 12
3.5 Step 5: Apply Controls Based on Security Classification 12

1 Introduction

Information is an essential resource that must be protected throughout its life cycle. However, not all pieces of information an organization holds have the same value and do not require the same level of protection. The categorization of information assets in information security is a process allowing the organization to assess the degree of sensitivity of its information, to determine the level of protection concerning the risks incurred in terms of availability, integrity, and confidentiality.

An organization will thus be able to take into account the degree of sensitivity determined to put in place measures enabling it to comply with its legal obligations, avoid financial losses as well as reputational risks and achieve its objectives with regard to its level of services and to increase the confidence of citizens and businesses in public services.

1.1 Impact Levels related to Information Assets of an Organization

The level of impact reflects the significance of the consequences that a breach in the security of an information asset can have on the organization and its customers or other organizations. These consequences can result in the organization's inability to:

- Fulfill its mission;
- Comply with laws, regulations, and contractual obligations;
- Preserve its brand image and that of the government;
- Maintain or enhance the confidence of customers and partners in the services offered;
- Respect the fundamental rights of individuals to the protection of personal information concerning them and their private life;
- Respect the protection of confidential information shared by the business entities concerning their business presence and competitive advantage;
- Contribute towards the functioning of third-party organizations that depend on its services.

The table below describes the levels of impact that public bodies can adapt to their context.

Impact Level	Description	
1	Low (negligible)	▪ Affects a line of business, i.e. a specific service/facility provided, in the organization.
2	Medium (moderate)	▪ Affects several areas of activity of the organization
3	High (severe)	▪ Significantly affects the quality of services essential to the population. ▪ Affects the image of the organization. ▪ Affects the activities of one or more other organizations. ▪ Affects respect for the fundamental rights of individuals to the protection of personal information concerning them and of their privacy, without harming the health, life, or well-being of these individuals. ▪ Affects respect for the confidentiality of the information shared by the business entities to the protection of their business presence and competitive advantage.
4	Very High (very serious)	▪ One or more services essential to the population cannot be provided. ▪ Endanger the health, life, or well-being of persons. ▪ Affects respect for the fundamental rights of individuals to the protection of personal information concerning them and their privacy and, as a result, endangers the health, life, or well-being of these individuals. ▪ Affects the government's branding, with or without publicity.

In addition, the impact levels expressed in terms of availability, integrity, and confidentiality are described in the table below.

Security Criteria	Impact Levels			
	Level 1 (Low)	**Level 2 (Medium)**	**Level 3 (High)**	**Level 4 (Very High)**
Availability	The disruption of access to or use of information assets has a negligible impact on the organization.	The disruption of access to or use of the information asset has a moderate impact on the organization.	The disruption of access to or use of information assets has a serious impact on the organization.	The disruption of access to or use of information assets has a very serious impact on the organization.
Integrity	The unauthorized modification or destruction of the information asset has a negligible impact on the organization.	Unauthorized modification or destruction of information assets has a moderate impact on the organization.	Unauthorized modification or destruction of information assets has a serious impact on the organization.	The unauthorized modification or destruction of information assets has a very serious impact on the organization.
Confidentiality	Unauthorized access or disclosure of information assets has a negligible impact on the organization.	Unauthorized access or disclosure of information assets has a moderate impact on the organization.	Unauthorized access or disclosure of information assets has a serious impact on the organization.	The unauthorized access or disclosure of information assets has a very serious impact on the organization.

2 Information Classification

Information Classification is system encompassing principles, methodology, tools, and framework for designating different categories to Information based on impact and value. There are numerous different definitions of Information Classification; however, all of these views have the following principles in common.

- It applies to all information assets across the organization (any type or size);
- It provides a basis for data sharing and accessibility policies across the organization;
- It supports Confidentiality, Integrity, and Availability (CIA) principles of Information Security;
- The classification should be done according to sensitivity and value of the information (but not limited to);
- The Framework should be simple to understand and administer;
- The value of information changes with time, regulatory requirements, and changing business environment;
- The classification should not be dependent or open to interpretation by different people; but rather a set of governing rules;
- Such classification needs to be done over the entire lifecycle of information;
- The Information Classification should include extended organization - department, business partners, contractors, other organizations, and citizens;
- Classification is not ownership of a single individual and impacts everyone; and
- The classification rules are dynamic and need constant upgrade

2.1 Assigning Information Classification

Every government client organization is responsible for ensuring that information assets have a classification that is authorized 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 delegated at the earliest possible opportunity and as soon as the originator or owner is aware of the sensitivity of the information asset.

In case of information assets that are externally generated, and not otherwise classified, the organizational officer who receives them should ensure that an owner and custodian are assigned and that the asset is incorporated into the organization‘s information asset registers as appropriate.

2.2 Altering Information Classification

Fundamentally, the security classification of any information may be altered only by the organization which has originally assigned the classification to that information (owner organization).

Security classification thought to be inappropriate should be queried with the organization which has initially assigned the classification or the organization now responsible. If the organization is abolished or merged, the organization assuming the former organization‘s responsibilities may alter the classification. For information that has been transferred into the custody of the Government Archive of Sri Lanka, it is a good practice if such information is also stored and handled by the security classification assigned to that information.

2.3 Duration of the Security Classification

Duration of security classification means the period up till which the information shall be deemed to be sensitive and should be handled and stored by security classification assigned.

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 human resource form may become ‘Confidential’ when complete or filled.

The duration of security classification can be specified in the following ways:

- The organization owning the information or assigning the security classification to information may settle a specific date or event for declassification based on an assessment of the duration of the information's sensitivity. On reaching the date or event the information should be automatically declassified;

- Declassification period of information can also be assigned in terms of a set period after the last action on an asset (e.g. six months after last use);

- If the organization assigning the security classification cannot decide a specific date or event for declassification, information should be marked for declassification at a pre-defined period as per applicable Government norms like 10 years from the date of the original classification;

- Organization assigning the security classification may extend the duration of security classification, change the security classification, or reclassify specific information only as per the protocols and guidelines for security classifying information;

- Information may be marked for an indefinite duration of security classification as well, and Cabinet documents are not included in such arrangements

2.4 Levels of Security Classification

Broadly, five levels (four classification levels plus —Unclassified) of security classification have been defined as

- Unclassified (White)
- Public **(Green)**
- Limited Sharing **(Amber)**
- Confidential **(Red)** and
- Secret **(Scarlet)**

2.4.1 Unclassified

All Government information, until such time they are evaluated and classified, must be allocated to the interim classification status —**Unclassified**. Any unclassified information should be treated similarly or higher to information classified as —Limited sharing. Prior authorization must be obtained from the information owner

to release **unclassified** material to the public (which is in effect changing the classification of the information).

2.4.2 Public

Any information which is easily available to the public, Government employees, organizations, regulators, project managers, support staff, and contractors including information deemed public by legislation or through a policy of routine disclosure can be classified as **"Public"**. This type of information requires minimal or no protection from disclosure. Examples of public information include:

- Government acts and policies;
- Organization contact persons;
- Information on public services provided to citizens by Government;
- Weather Information; and
- Advertisement for job postings

Note:

While Public information assets have no confidentiality requirements it is still important to ensure their accuracy and completeness (integrity) prior to release. For example, information published on a website must be protected from being tampered with or changed. Information Classification Framework does not discuss controls that ensure the integrity and availability of public information, and steps must be taken by organizations to ensure Public information assets remain available within business needs and are not tampered with.

Some information assets intended for public consumption may have confidentiality requirements before their release (for example, budget papers). In this case, the point at which the information asset will be reclassified to the Public must also be indicated.

Information assets must be specifically classified as public before their release. Public information should at all times be approved as such by the information owner. Where information assets have not yet been classified, they should be treated as unclassified and not as public.

2.4.3 Limited Sharing

Information is security classified as **"Limited Sharing"** when compromise of information may lead to minor probability of causing limited damage to the Government of Sri Lanka, commercial entities, or members of the public. Unauthorized disclosure of this information will cause negligible or no damage to

internal security, Sri Lankan forces, or Sri Lanka‘s foreign relations. Examples of Limited sharing information are:

- Organization processes and information;
- Personal information[1] of citizens;
- Confidential information of business entities;
- Minutes of meetings and file notes of Organizations;
- Government evaluation on a company’s products; and
- Inventory data.

2.4.4 Confidential

Information is classified as **“Confidential”** when compromise of information may lead to a high probability of causing damage to national security, internal stability, national infrastructure, forces, commercial entities, or members of the public.

In the case of material marked ‘CONFIDENTIAL,’ the information asset is subject to disclosure which may be limited or prohibited.

Examples of Confidential information are:

- Personal case files such as benefits, program files, or personnel files;
- Tax returns or financial health of the organization;
- Sharing of personal health information of individual;
- Trade secrets; and
- Salary information

2.4.5 Secret

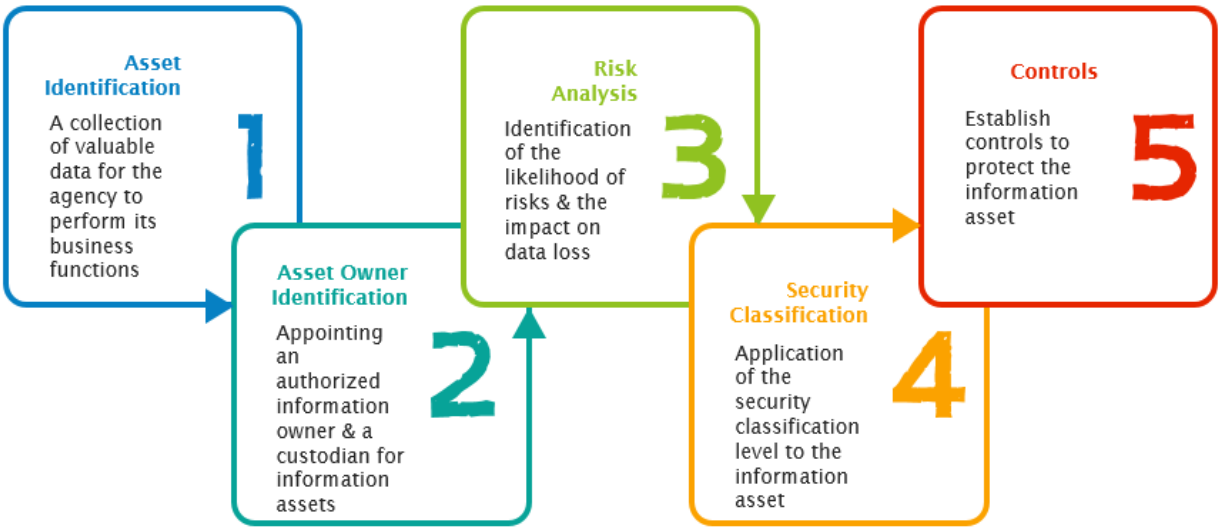
Information is classified as **“Secret”** when compromised could cause serious damage to national security, Government, nationally important economic and commercial interests or threaten life. It could also raise international tension and seriously damage relations with other governments, shut down or substantially disrupt significant national infrastructure and seriously damage the internal stability of Sri Lanka or other countries. Examples of Secret information are:

- Details of sex offenders and victims;
- Criminal investigations for major crime;
- Data related to foreign affairs;
- Cabinet documents; and
- Provincial Budget prior to public release

[1] Personal information is governed by the Data Protection Act No.19 of 2022

3 The Information Classification Process

It is necessary to ensure that the process is understood to be an organic process, that is, that information 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.



3.1 Step1: Identify Information Assets

Information assets are defined as an identifiable collection of data, stored in any manner and recognized as having value for enabling an agency to perform its business functions, thereby satisfying a recognized 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
- 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 Information Security Classification 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 is more properly described as Information and Communication Technology (ICT) assets. ICT assets which are not considered as information assets include:

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

3.2 Step 2: Identify the owner of the Information Assets

Each organization is responsible for ensuring that information assets have a security classification that is authorized 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.

Note:

Information owners define the policy which governs the information assets of an organization, for example determining the classification of information assets. An owner will often delegate the operational responsibility for information assets to a custodian, who applies controls that reflect the owner's expectations and instructions such as ensuring proper quality, security, integrity, correctness, consistency, privacy, confidentiality, and accessibility of the information assets.

3.3 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 needs 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.

3.4 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.

3.5 Step 5: Apply Controls Based on Security Classification

Appropriate controls, as prescribed in the 'National Data Sharing Policy', must be applied to ensure that protection is given to information assets commensurate with the security classification level that has been determined.