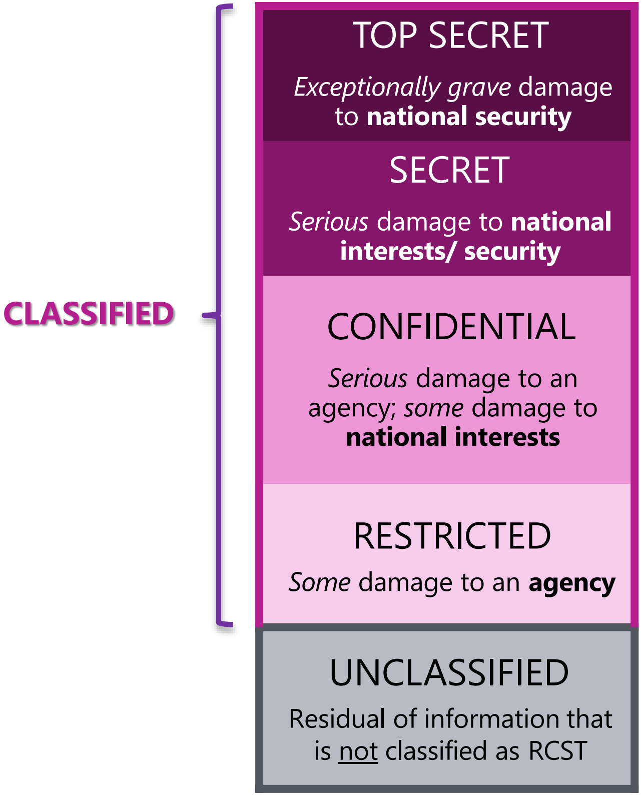
2019

Sharing on:

Guide to Right Classification

OLD RCST Framework: does not define UNCLASSIFIED; data was over-classified to RESTRICTED or CONFIDENTIAL



CLASSIFIED

TOP SECRET

Exceptionally grave damage to **national security**

SECRET

Serious damage to **national interests/ security**

CONFIDENTIAL

Serious damage to an agency; *some* damage to **national interests**

RESTRICTED

Some damage to an **agency**

UNCLASSIFIED

Residual of information that is not classified as RCST

Official Information:

"All info that public officers acquire (except that which is already openly or publicly available), generate or cause to be generated in the course of their duties"

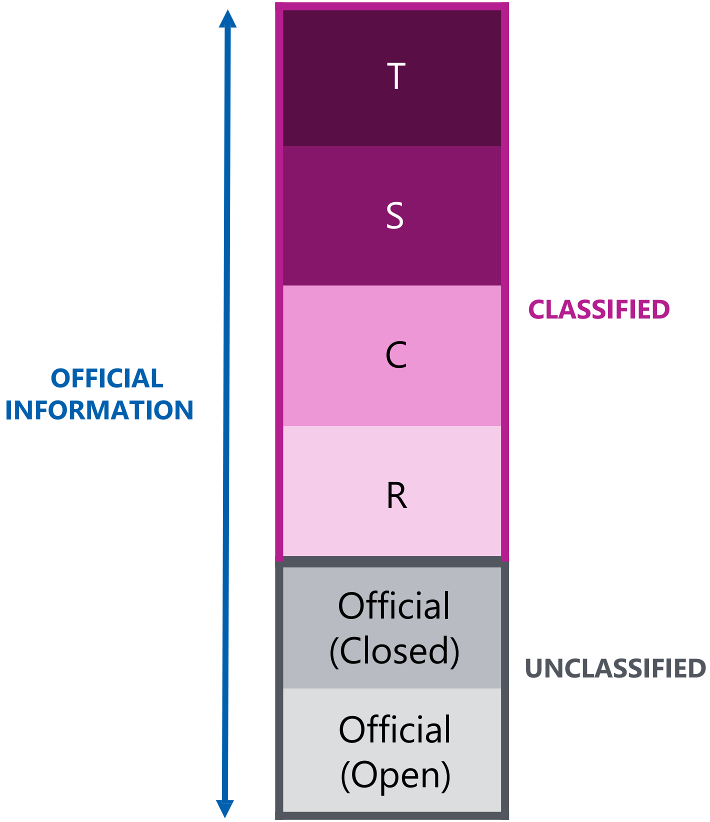
Classified Information:

"Official information that has been assigned a security classification, based on the potential damage or negative consequence of unauthorised disclosure"

Source: From ISD Green Book

Right Classification Guide: Part I – Security Classification

Refer to the classification of official information and systems based on the RCST Framework set out in the Green Book.



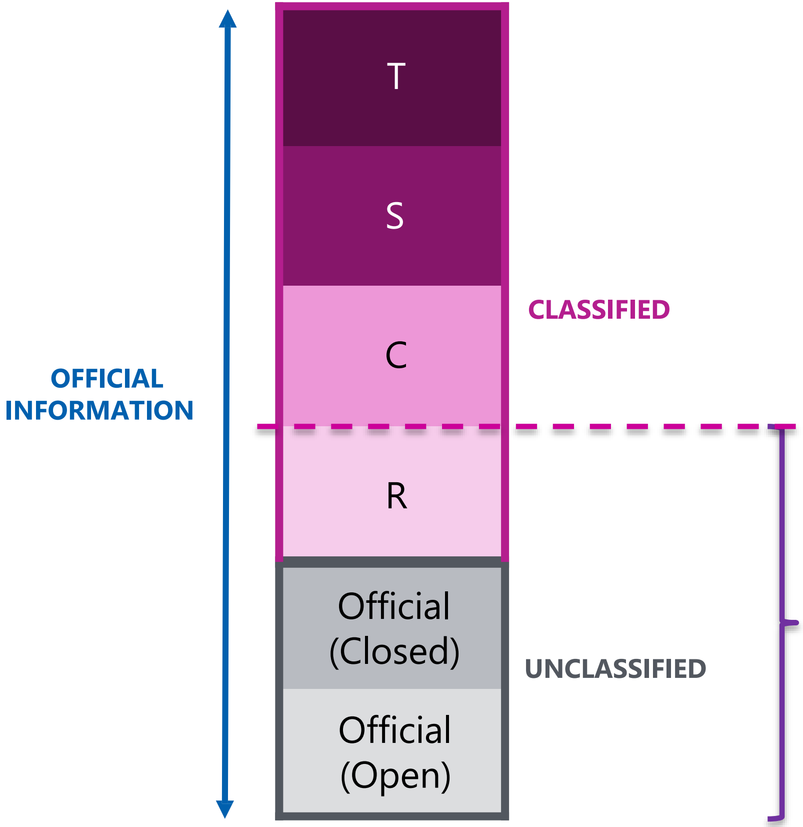
To facilitate right-classification of Govt systems under the RCST Framework, two new markers have been introduced to further differentiate official information that are Unclassified:

1. **Official (Closed)**
   The unauthorised disclosure of information in this category will have negligible or no impact to the agency functions, national interests or national security. However, such information is not disclosed to the public in the normal course of duty.

2. **Official (Open)**
   Similar to Official Closed, except information is disclosed to the public domain. An example is information found on Data.gov.sg (open data).

Right Classification Guide: Part I – Security Classification

Information Asset / Data Classification (for all IHLs)



In all IHLs (5 Polytechnics and ITE), there are only 3 levels of classification under RCST framework, namely:

- **R : Restricted**
- **O(C) : Official (Closed)**
- **O(O) : Official (Open)**

Right Classification Guide: Part I – Security Classification

To determine the system's security classification, we need to answer the questions below.

Question 1

Will any unauthorised disclosure of information in this system likely cause –

- Some disadvantages in negotiations affecting national interests; or
- Some disruption to national security; or
- Some disruption to services essential for public safety or maintenance of public order; or
- Some disruption to the financial or economic system in Singapore?

❑ **Yes**

System is **Confidential**

Examples: Criminal Record Office System, Diplomatic Bag System, Trade Database System

❑ **No**

Please proceed to Question 2.

Right Classification Guide: Part I – Security Classification

To determine the system's security classification, we need to answer the questions below.

Question 2

Will any unauthorised disclosure of information in this system likely cause a disruption to your agency's critical process resulting in its inability to discharge its functions?

❑ **Yes**

System is **Confidential**

Examples:

Police Coast Gurad AEGIS System

CUSTOMS Business Risk Profiling System

Integrated Criminal Case Filing and Management System

Customs Intelligence and Investigation System

❑ **No**

Please proceed to Question 3.

Right Classification Guide: Part I – Security Classification

To determine the system's security classification, we need to answer the questions below.

Question 3

Will any unauthorised disclosure of information in this system likely cause a disruption to your agency's process resulting in a hindrance to discharge its functions?

❑ **Yes**

System is **Restricted**

Examples:

Port Traffic Management System

Integrated Stamp Duty System

HR Systems

❑ **No**

Please proceed to Question 4.

Right Classification Guide: Part I – Security Classification

To determine the system's security classification, we need to answer the questions below.

Question 4

Do members of the public have to access to the information in this system?

❑ **Yes**

Please proceed to Question 5.

❑ **No,** this system is completely inward-facing.

System is **Official (Closed)**

Examples:

Office Administrative Systems/Staff Directory

Staff Suggestion System

Central Stationery Management System

Room Booking System

Right Classification Guide: Part I – Security Classification

To determine the system's security classification, we need to answer the questions below.

Question 5

What access do members of the public have to the information in this system?
(For example, a portal that the public can use to search for information)

□ **Full**

System is **Official (Open)**

Examples:

Archival Systems such as Parliamentary Reports

PMO-PO Corporate Website

□ **Partial**

System is **Official (Closed)**

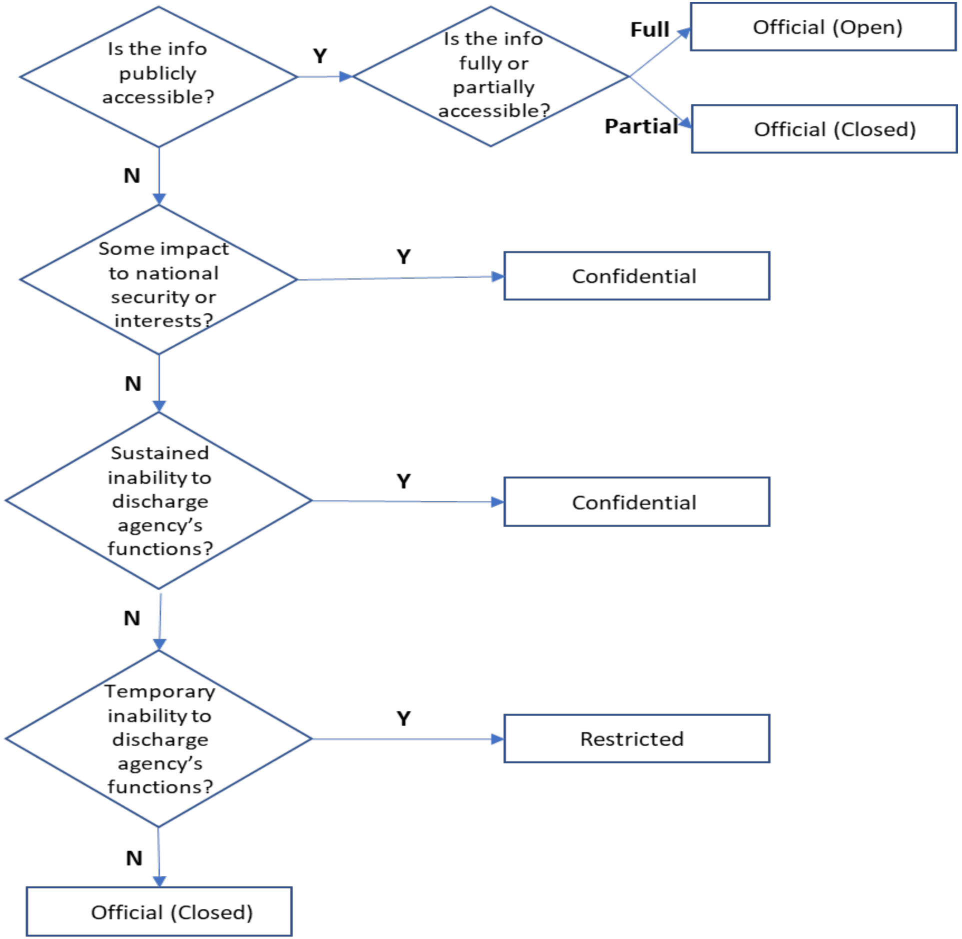
Examples:

Online Feedback Platforms

Portals for Application of Services, etc.

Facility Booking Systems (e.g. for Sports, etc.)

Decision Tree for Security Classification


Is the info publicly accessible?
Y
Is the info fully or partially accessible?
Full
Official (Open)
Partial
Official (Closed)
N
Some impact to national security or interests?
Y
Confidential
N
Sustained inability to discharge agency's functions?
Y
Confidential
N
Temporary inability to discharge agency's functions?
Y
Restricted
N
Official (Closed)

Right Classification Guide: Part II – Sensitivity Categorisation

The Information Sensitivity Framework (ISF) considers the impact of unauthorised disclosure of entity data, which comprises data on individuals and business.

SENSITIVITY Categorisation	INDIVIDUAL	BUSINESS
Sensitive High ***Serious*** damage to an individual or business (e.g. incriminating information), if leaked.	Causes <u>serious physical, financial, or sustained emotional injury or social stigma to </u>the individual E.g.: Loss of life or physical harm; loss of employability, reputation and insurability; case information that reveals the identity of victims of sexual assault etc., criminal or investigative records, etc.	Causes <u>sustained financial loss</u> E.g.: Inability to conduct normal business operations, significant and irreversible loss of competitive advantage, major damage to reputation.

Right Classification Guide: Part II – Sensitivity Categorisation

The Information Sensitivity Framework (ISF) considers the impact of unauthorised disclosure of entity data, which comprises data on individuals and business.

SENSITIVITY Categorisation	INDIVIDUAL	BUSINESS
Sensitive Normal ***Some*** damage to individual or business, if leaked.	Causes temporary and minor emotional distress or disturbance to the individual E.g.: Locational information, photographic images, etc.	Causes a reduction in competitiveness or a compromise of business interests E.g.: Loss of potential business opportunities, some damage to reputation.

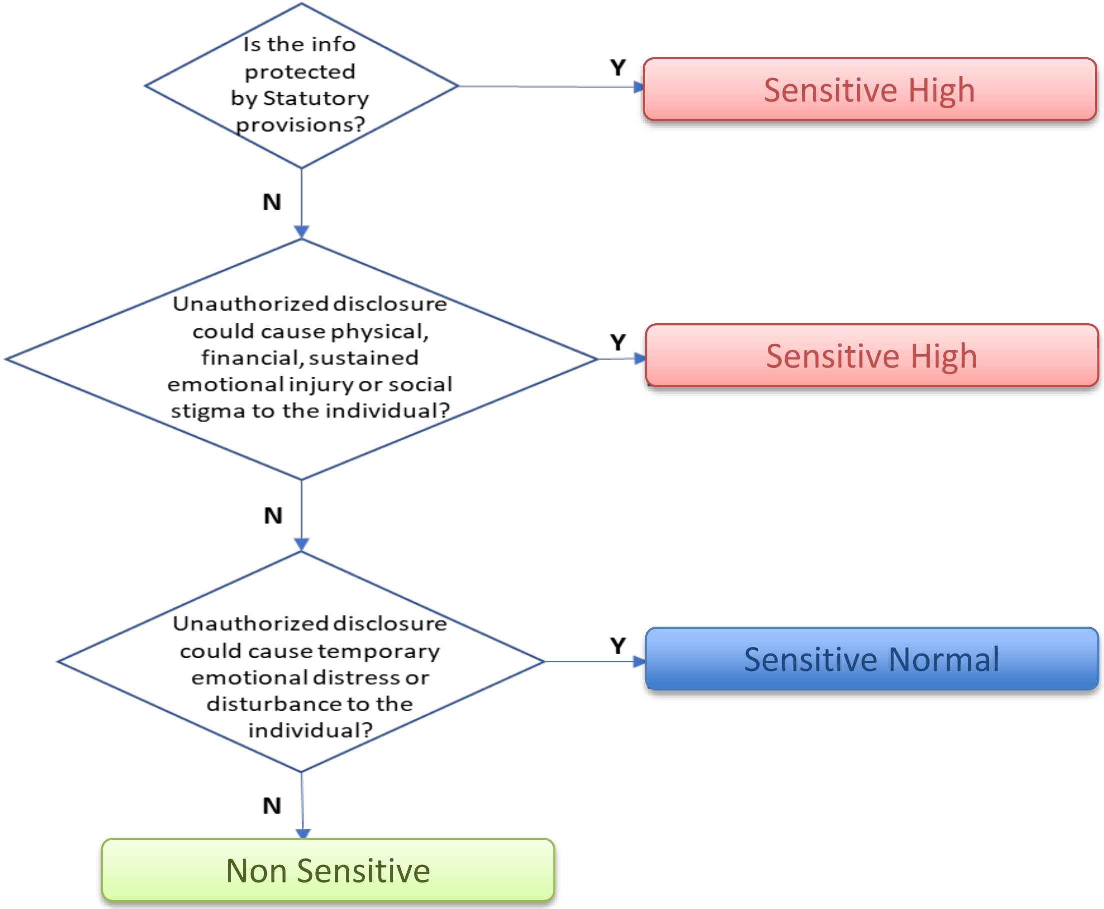
Right Classification Guide: Part II – Sensitivity Categorisation

The Information Sensitivity Framework (ISF) considers the impact of unauthorised disclosure of entity data, which comprises data on individuals and business.

SENSITIVITY Categorisation	INDIVIDUAL	BUSINESS
Non-Sensitive ***Negligible or no*** damage to an individual or business, if divulged.	Does not cause physical, financial, or emotional injury to the individual; OR in personal information that is socially expected to be openly available.	Does not impact a business' processes or operations; OR is Business information that is socially accepted as openly available.

Restricted

Decision Tree for Information Sensitivity Classification



Is the info protected by Statutory provisions?
Y
Sensitive High
N
Unauthorized disclosure could cause physical, financial, sustained emotional injury or social stigma to the individual?
Y
Sensitive High
N
Unauthorized disclosure could cause temporary emotional distress or disturbance to the individual?
Y
Sensitive Normal
N
Non Sensitive