وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

CIIP Department, Cyber Security Sector

Guidelines for Data Classification & Data Labelling

Step By Step Approach

Version: 1.0
Published: June 2021
Classification: Public

Legal Mandate

Cabinet Decision No. 26 for the Year 2018 on establishing the Cyber Security Sector within MOTC, and the **Emiri Decision No. 8 for the Year 2016** that sets the **mandate for MOTC** provide that MOTC has the **authority to supervise, regulate and develop the sectors of Information and Communications Technology** (hereinafter "ICT") in the State of Qatar in a manner that is consistent with the requirements of national development goals, with the objectives of creating an environment suitable for fair competition; supporting the development and stimulating investment in these sectors; securing and raising the efficiency of the information and technological infrastructure; implementing and supervising e-government programs; and promoting community awareness of the importance of ICT to improve the lives of individuals and the community and build a knowledge-based society and digital economy.

Article 22 of the Emiri Decision No. 8 of 2016 stipulates the **role of MOTC** in protecting the **security of the National Critical Information Infrastructure by proposing and issuing policies and standards and ensuring compliance.**

This guidance for Data Classification has been developed taking into consideration current applicable laws of the State of Qatar.

In the event a conflict arises between this document (specific provision or clauses) and the laws of Qatar, the latter (law), SHALL take precedence. Any such term (specific provision or clauses), to that extent SHALL be deemed omitted from this document, without affecting the remaining provisions of this document. Amendments in that case shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar.

Objective of this Document

The objective of this document is to provide guidance to the stakeholders and help them understand the Data Classification, and the proposed Data Labelling in context of the Data Life cycle and implement it within their organization in line with the National Information Assurance Policy v2.0.

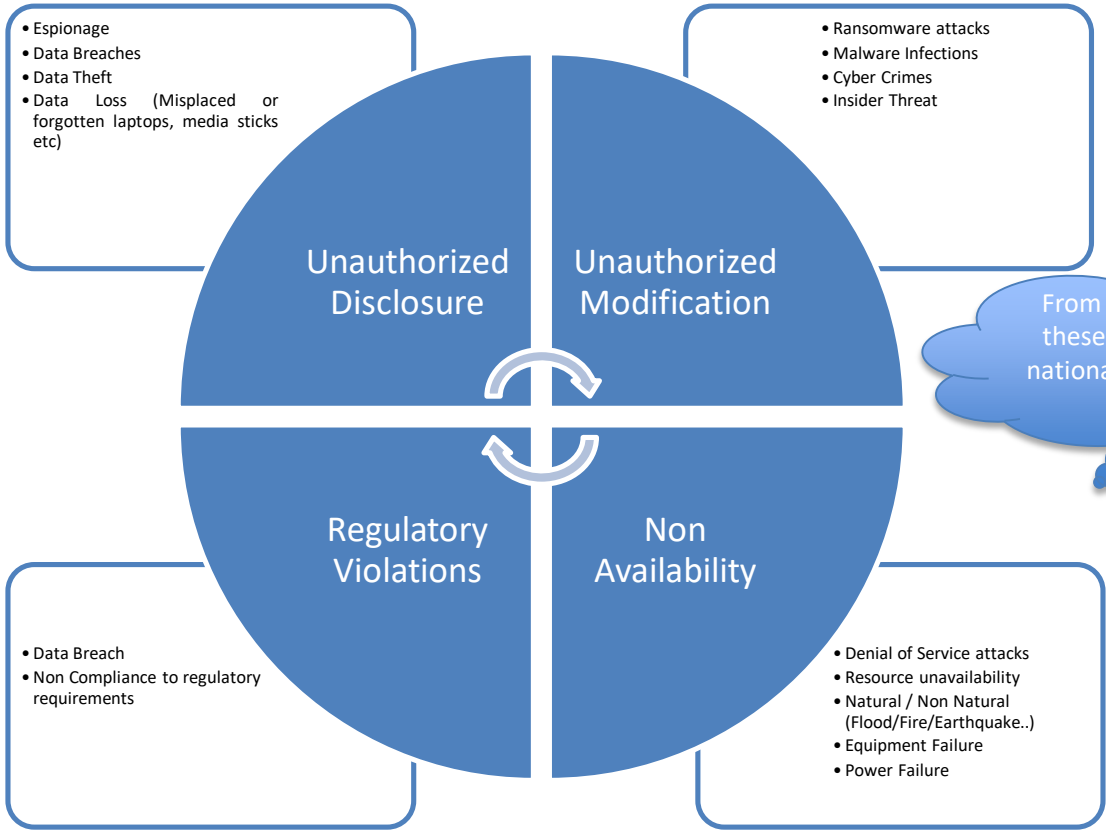
This document complements the National Information Assurance Policy v2.0 and must not be used in isolation.

The Need for Data Life Cycle Management

Why do we need to manage our Data

- ✓ Have a helicopter view of your business data.
  - ❑ Identify your critical data (crown jewel)
- ✓ Manage your resources optimally.
  - ❑ Know where to put in your resources/ efforts
- ✓ Meet Business expectations
  - ❑ Secure your business data and maintain competitive edge in the market.
  - ❑ Provide assurances to your customers and stakeholders
- ✓ Meet Legal and Regulatory expectations
  - ❑ Comply with the relevant regulatory requirements.

Top Risks and Threats to Data



From a national perspective, these could have impacts on national security and economic stability.

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Where to Begin?

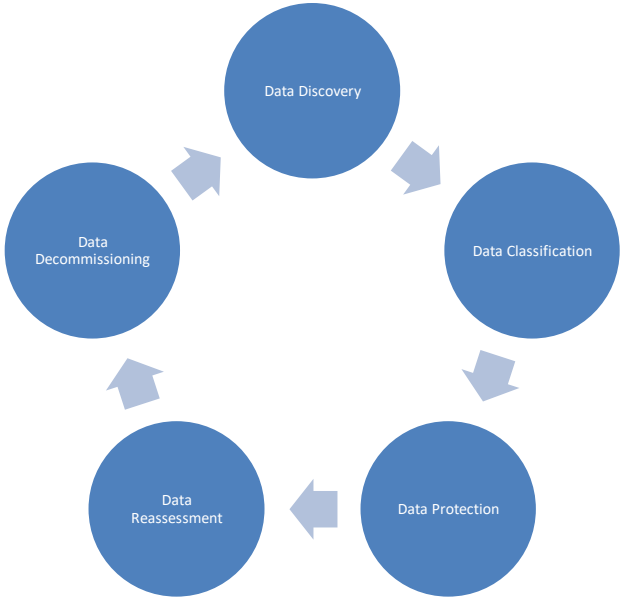
Understand the Process

Understand the Data Life Cycle

Data is not static, it undergoes changes in its life cycle and its value may change over a period of time. At some point it may cease to have any value or may lose its value or maybe forced to an end of life, eventually leading to destruction and disposal of data.

Key steps in the Data Lifecycle include:

- ✓ Data Discovery
- ✓ Data Classification
- ✓ Data Protection
- ✓ Data Reassessment
- ✓ Data Decommissioning



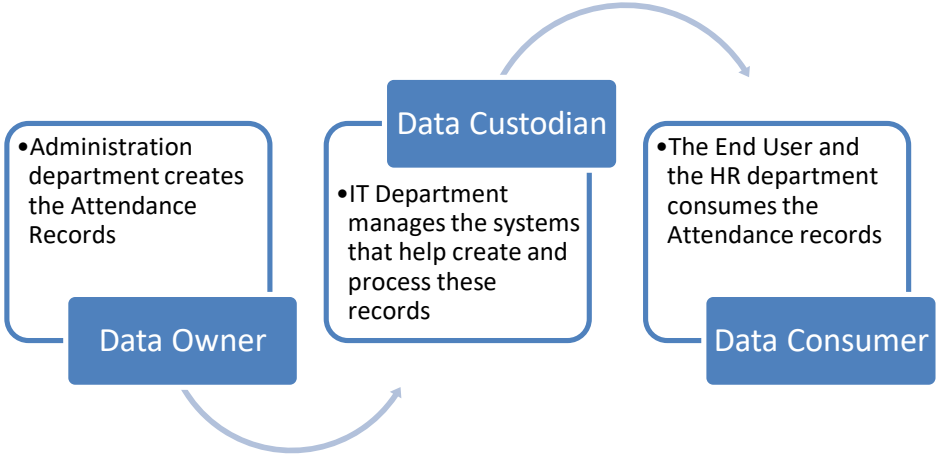
Data Management Roles

The following example will help you understand the various roles in the Data Management Lifecycle.

Data Owner: The Process/Service owner whose process creates the Data is the Owner of the Data. The Administration department will generate the attendance records of individual employees. So, Administration Manager or the Administration function owns the Attendance records. The Data owner also acts as the Labeling authority, defining the labels for various categories / types of data created by the service/process.

Data Custodian: These attendance records are stored, processed and generated through a Time and Attendance management system, as such the IT department which provides, supports and facilitates these system becomes the Data Custodian. The Data Custodian facilitates the technology labelling the data.

Data Consumer: Eventually the Attendance records will be used by the HR Department to process the salary of the user and by the end user himself to verify and maintain his attendance records, so they become the Data Consumer



Data Management Supporting Roles

The following example will help you understand the various supporting roles in the Data Management Lifecycle.

Data Champion: is a person who is generally trained and understands the business and data and is assigned the duties to help the different stakeholders within the organization to support and drive data classification efforts as a part of the organization's overall data strategy.

Data Creator: The Process/Service owner whose process creates the Data is the Owner of the Data. However, the data per se may be created by various members of the department. For example, the various clerks and support staff within the Administration department will be generating the attendance records of individual employees. So, Administration Manager or the Administration function owns the Attendance records, whereas the Administration clerks or the support staff create/generate those records. The Data creator is also responsible for ensuring that the data is labeled upon creation.

Data Auditors: The data auditor reviews the data owner's assessment of the classification and determines if it's in line with business, regulatory, and other corporate requirements. The data auditor also reviews feedback from data users and assesses alignment between actual or desired data use and current data-handling policies and procedures.

Data Discovery

Data Discovery consists of two steps:

1. Discover where does the Data come from.
2. Creating and inventory of the Data

Discover Data Source:

Understand the sources of your data (Business Processes).

Know where all your data is located, stored and processed.

- **Data Creation:** This is creation of records/data from scratch.

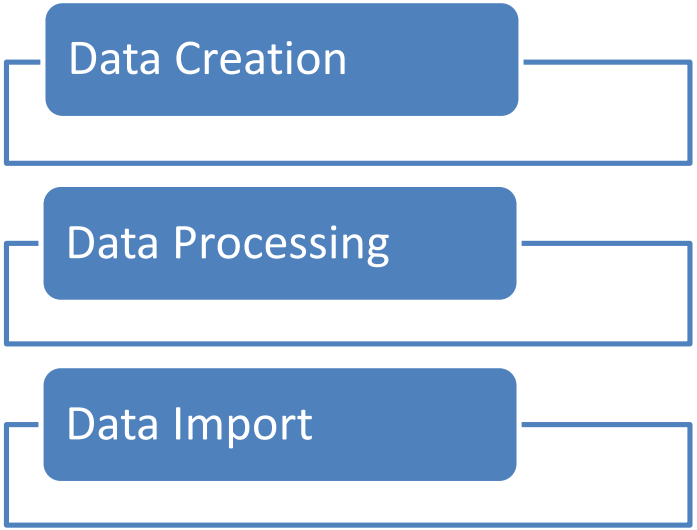
  Examples: Creating a new document in a Word Processing application, Writing a new email, An event log created by a system etc.

- **Data Processing:** This is processing of existing records by an application or a system to create a new record/data.

  Examples: Creating a monthly attendance report or a Salary slip based on the daily attendance records, reply to an incoming email, An alert created by a SIEM solution based on the event logs etc.

- **Data Import:** This is ingesting data from an external data source (media and/or system).

  Example: Importing files from a USB, machines sending logs to a central syslog/SIEM server, records from an attendance system being sent to the payroll system etc.



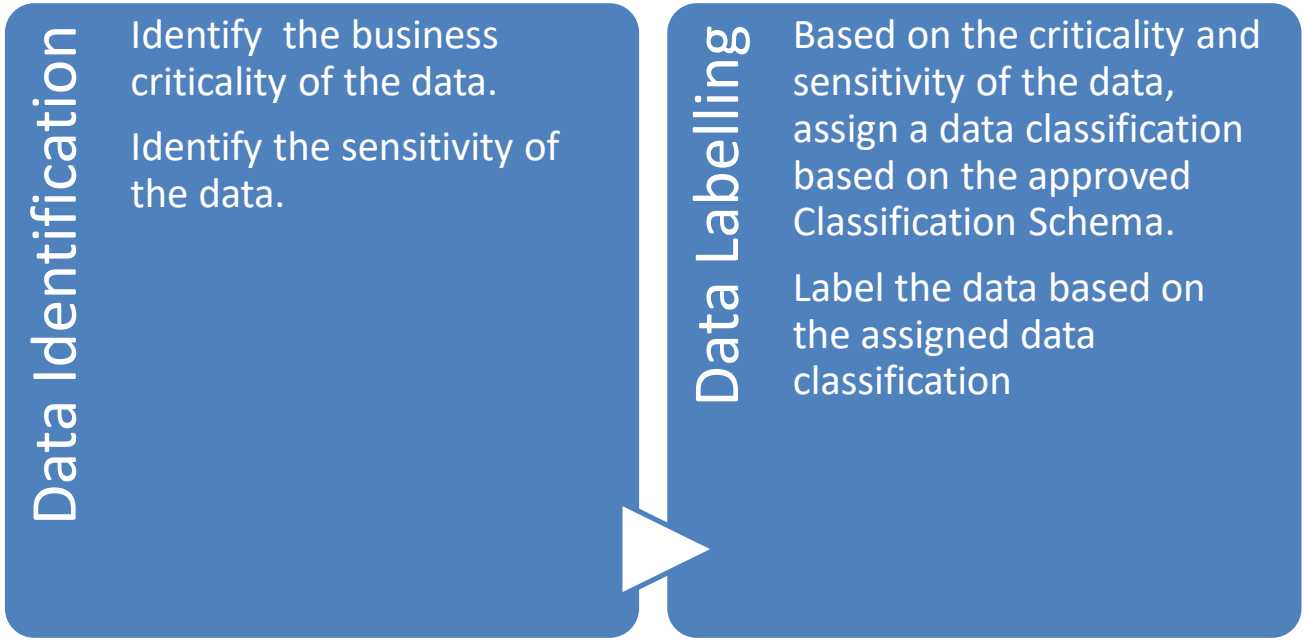
Data Discovery

Data Inventory:

This is a formal process of making a recorded inventory of various data sets that you have within your organization.

As with any other inventory, the process should record the Ownership of the Data Assets, including associated processes and systems.

Data Classification



Data Labelling should occur whenever data is created, or undergoes transformation, or when the classification changes, or when it reaches an end of life.
*For retro (historic) data, an exercise needs to be carried out to integrate it with the Enterprise Data Management system.

NIAP Model for Classification

Attached is the proposed classification model from National Information Assurance Policy v2.0

The Classification is based on the **C**onfidentiality, **I**ntegrity and **A**vailability attributes of the data.

Data is classified as **L**ow, **M**edium, or **H**igh based on the overall classification and is treated accordingly during its life cycle.

The Data Label is however based on the **C**onfidentiality attribute of the data.

		A0	A1	A2	A3
	C0		L	M	H
	C1	L	L	M	H
	C2	M	M	M	H
I0	C3	H	H	H	H
	C0	L	L	M	H
	C1	L	L	M	H
	C2	M	M	M	H
I1	C3	H	H	H	H
	C0	M	M	M	H
	C1	M	M	M	H
	C2	M	M	M	H
I2	C3	H	H	H	H
	C0	H	H	H	H
	C1	H	H	H	H
	C2	H	H	H	H
I3	C3	H	H	H	H

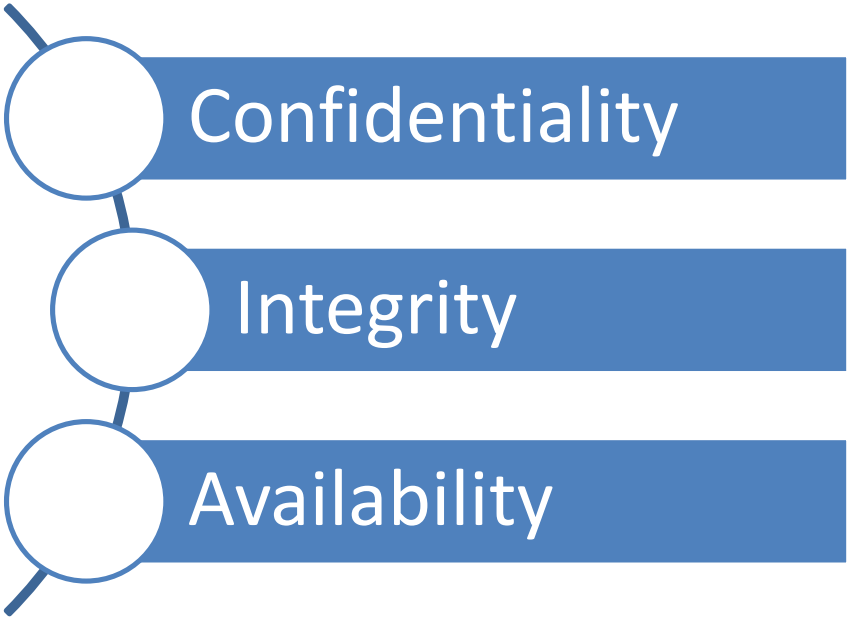
Data Protection

Based on the criticality and the sensitivity of your data, you will need to implement appropriate controls to protect the Confidentiality, Integrity and Availability of your data.

The controls chosen shall also be governed by the state of data vis-à-vis Data in Transit, Data in Rest, and Data in Use.

NIAP proposes Baseline Controls for all data assets, data assets that have been classified as M or H, need additional controls commensurate and corresponding the attributes (C or I or A) that led to the asset being classified as M or H

Data classification provides you with this visibility and understanding and helps you allocate your resources (time, efforts and manpower) accordingly to ensure an optimum Return on your Security Investment (ROSI)



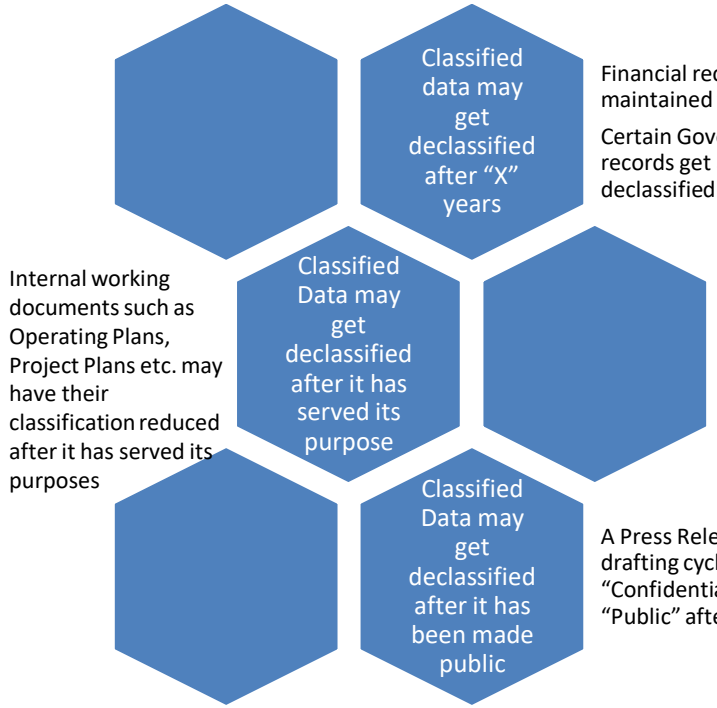
Data Reassessment

The value of data may change from time to time, based on various factors such as processing cycle, time, right to usage, applicability to business etc.

This may in turn impact the classification of the data.

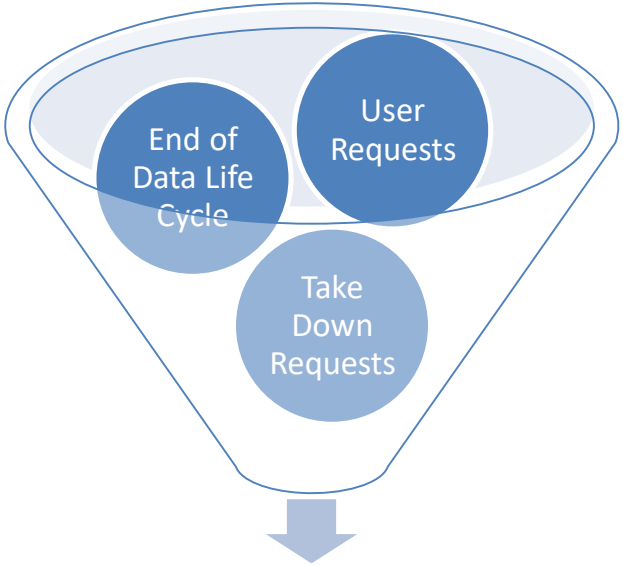
From time to time, businesses (users) should assess and validate the classification of the data. On a minimum such assessments should be done annually and/or at the end of defined data retention period.

Corrective actions in terms of controls applied will need to be taken based on this reassessment



Data Decommissioning

1. Data is usually disposed of in two cases:
   - ❑ End of Data Life Cycle: It is not advisable to maintain data forever. Once the data has served its purposes, it should be Decommissioned and purged from the systems to complete its life cycle. Agencies should in consultation with their legal department, define Data Retention policies within their organization. The Data Retention period should take into consideration any regulatory requirements, corporate requirements, contractual requirements, and legal requirements if any.
   - ❑ Legal Requests: At times you may have a legally binding reason to delete data from your systems. These could be due to:
     - ✓ User Requests: Under Privacy legislations such as Qatar PDPPL and GDPR, users can request organizations to delete their personal data from their systems
     - ✓ Takedown Requests: Knowingly or Unknowingly, the organization may have illegal, unlicensed or copyrighted information within their systems which may constitute a breach of law. Such information when identified, should be removed with immediate effect.
2. Organizations should evaluate and implement controls if necessary to seek approval, prior declassification of any data.
3. Users should know and practice secure disposal methods based on the classification of data.



Data Decommissioning

In Summary

Data Lifecycle	People	Process	Technology
Data Discovery	Users to be provided with the necessary Training & Awareness on Data Classification. Users to classify/declassify data based on the organization's approved Data Classification schema and the guidance provided by the Data Owner. Roles and Responsibilities related to Data Management should be clearly communicated to all users. Users should comply with the organization's policies, standards and guidelines. Users should read, understand, sign and comply with the Non Disclosure and Confidentiality agreements	Business Impact Assessment exercise to identify and document business processes within an organization. OBASHI or any similar model to map information assets within a process Data Classification process that covers Data Inventory, Data Identification and Data Labelling Data Reassessment Process to revalidate the assigned classification values Data Decommissioning process that covers Data Sanitization, Data Disposal Incident Management Process that covers Incident Reporting, Incident Handing Business Continuity Management Process that covers Crisis Management	Data Discovery Tools (Data At Rest, Data In Transit and Data In Use) Data Classification Technology Data Protection (These includes amongst others Data Leakage Protection (DLP), Data Rights Management (DRM), Encryption, Access Control Solutions etc.) Data Monitoring Tools (These includes amongst others Email/Web gateways, DLP, DRM, etc.) Data Disposal Tools such as Degausser, Data Sanitization and Disposal tools, Data (Media) Destruction tools etc.
Data Classification			
Data Protection			
Data Reassessment			
Data Decommissioning			

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Understood the Data Life Cycle

What Next?

Data Classification – Schema

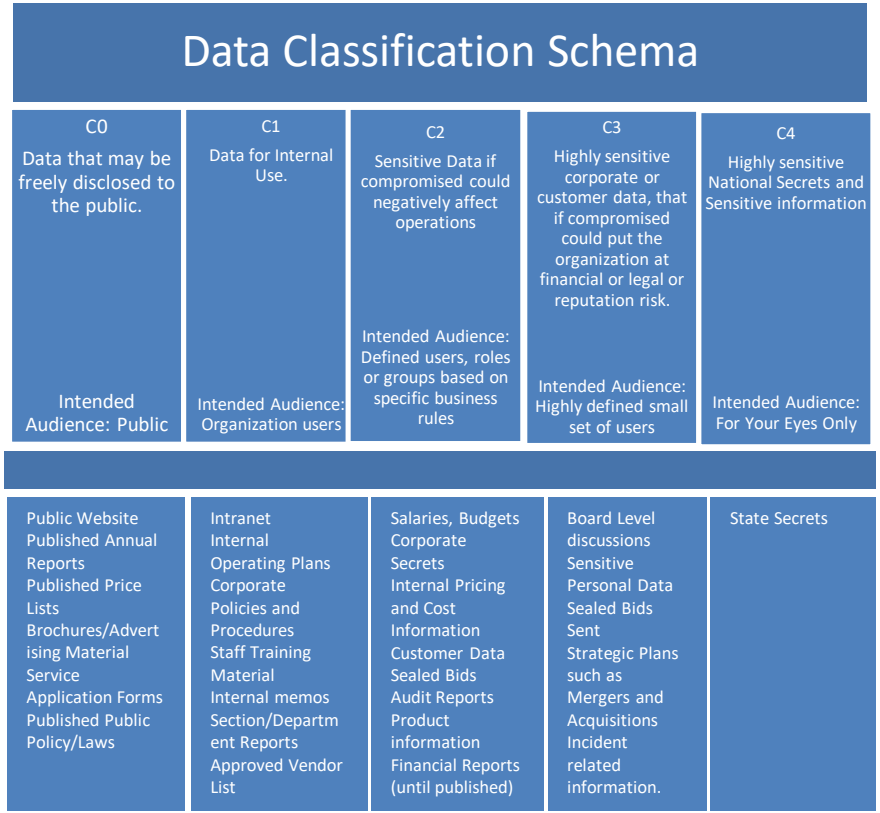
Each organization will create an Internal Policy that will mandate a Data Classification Schema in line with the National Information Assurance Policy v2.0

On a Minimum Agencies will implement a 4 level schema that will classify information from C0 – C3.

Government Agencies will implement a 5 level schema that will classify information from C0 – C4

C1 will be the Default classification for data that is not labelled.

C4 will be the classification designated for National Secrets.



Data Classification – Labels

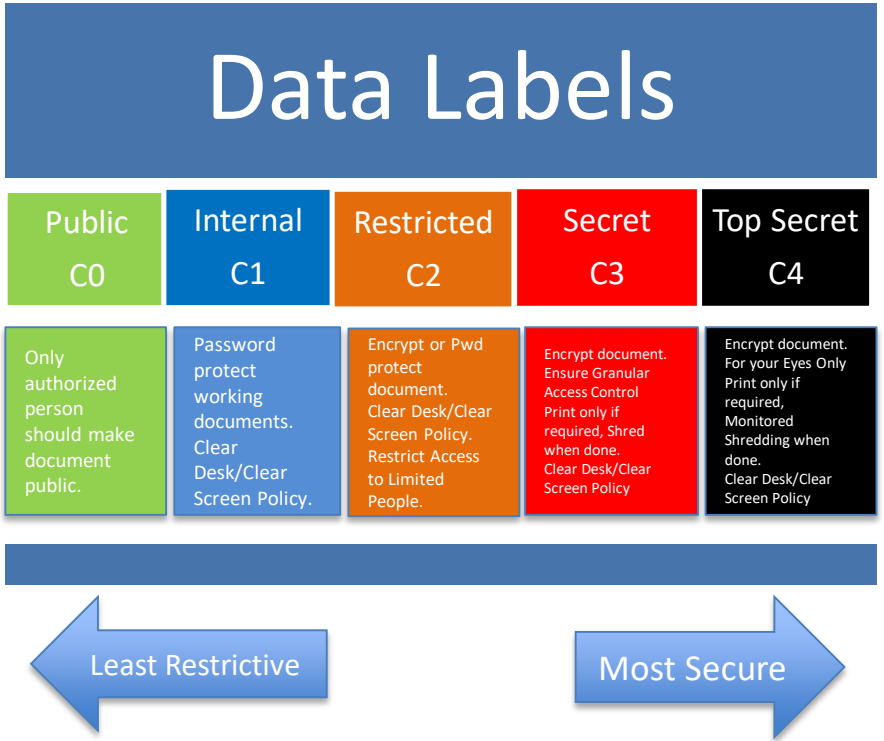
The Recommended labels to be used are as follows:
C0 → Public
C1 → Internal
C2 → Restricted
C3 → Secret
C4 → Top Secret

Organizations will create the necessary awareness and train their employees to use this classification schema.

Organizations will implement the necessary technology to automate and simplify the efforts involved in Data Classification. These includes tools to Discover and Inventory your Data Assets, tools to Classify and Label your Data

Where possible, visible including but not limited to color coding, shall be used to label the data.

Tools should also enable you to use meta labels



Data Classification – Next Steps

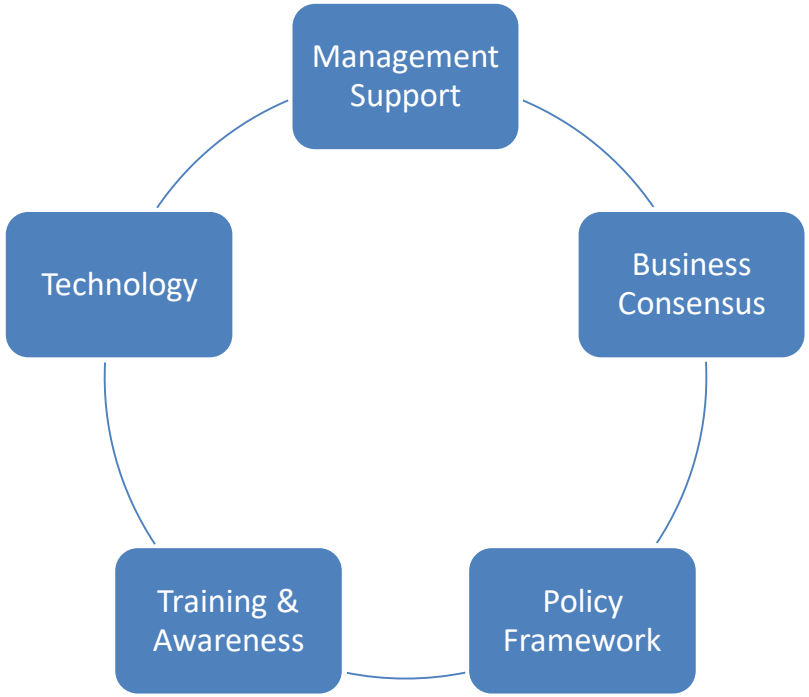
Management Support: Get support from the Highest management level in the entity (Minister, CEO, etc).

Business Consensus: Create a working group/committee comprising of various business units in the organization to drive and manage this initiative.

Policy Framework: Define and implement the necessary policies and procedures related to Data Classification.

Training & Awareness: Create awareness and training around Data Classification for all users in the organization.

Technology: Identify and evaluate the various technical solutions available in the market to suit your organization



Areas of Challenge

Data Discovery: In today's age of BYOD and Remote working an organization has lost its sense of perimeter. Data could reside anywhere on the cloud (private or public), enterprise servers, user desktops, user mobile devices, user's cloud services, floating storages (USBs) etc. The ability to discover your enterprise data on all such silos is a huge challenge.

Data Control: An organization's control and powers to be able to reach out to data stored on user's personal devices and be able to protect it.

Data Labelling: The technology controls and ability to be able to label data, consistently and cohesively, agnostic of the media and the system it resides in/on. Example: Ability to label the email on the system, when it is printed and when it is sent out of the organization to a different mail server.

Data Reassessment: The ability in terms of the process and the technology to be able to consistently and cohesively reassess the data from time to time to assess and validate its classification. Example: Ability to declassify the data available as a backup on a tape drive.

Data Decommissioning: The ability to decommission the data consistently and cohesively across all mediums and systems. The challenge is acute for ad-hoc "Take Down: requests. Example: A user withdrew his consent for a certain data that was collected. In order to comply with such requests, you need to ensure that the user's data is removed from your production systems, backups and from all third parties that you shared the data with.

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Thank You

For any queries or clarifications email us at ciip@qcert.org