الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

NATIONAL DATA CLASSIFICATION POLICY

[IAP-NAT-DCLS]

MAY 2023

VERSION 3.0

VERSION 3.0

TOWARDS A SECURE CYBER SPACE

"DISCLAIMER LEGAL RIGHTS"

National Cyber Security Agency (NCSA) has designed and created this publication, titled "National Data Classification Policy - V 3.0", in order to help Organizations decide on classification of its data.

NCSA is responsible for the review and maintenance of this document.

Any reproduction of the present document either in part or full and irrespective of the means of reproduction; shall acknowledge NCSA as the source and owner of the "National Data Classification Policy".

Any reproduction concerning this document with intent of commercialization shall seek a written authorization from the NCSA. NCSA shall reserve the right to assess the functionality and applicability of all such reproductions developed for commercial intent.

The authorization from NCSA shall not be construed as an endorsement of the developed reproduction and the developer shall in no way publicize or misinterpret this in any form of media or personal / social discussions.

DOCUMENT CONTROLS

Document Details

► **Document ID**	IAP-NAT-DCLS
► **Version**	V3.0
► **Classification & Type**	Public
► **Abstract**	This document is intended as a policy to set the foundation of Data Governance within government and critical sector organizations in Qatar, as also to create a unified Data Classification scheme to facilitate information exchange within Qatar.

Review/Approval

Name	Dept./Role	Reviewed/Approved	Version	Date
Director of National Cyber Governance and Assurance Affairs	National Cyber Governance and Assurance Affairs		**3.0**	May 2023

Revision History

Version	Author(s)	Revision Description	Date
1.0	ictQATAR	Published	January 2010
2.0	MOTC	Published	February 2014
3.0	NCSA – National Cyber Governance & Assurance Affairs	Published	May 2023

"LEGAL MANDATE(S)"

The Amiri Decree No.1 for 2021 setting the establishment of National Cyber National Cyber Security Agency (NCSA), aims to maintain and regulate national cyber security and to enhance and protect the vital interests of the state in the face of cyber threats, Article No. (3) of the law, is concerned with developing and updating policies, governance mechanisms, standards, controls and guidelines necessary to enhance cyber security in coordination with the concerned authorities, and circulating them with the relevant authorities and follow-up commitment to them.

Within this context, this National Data Classification Policy has been developed which aims to regulate and govern the data classification scheme used by organizations in the State of Qatar. The policy identifies the basic principles that will help in understanding the data classification and governing the important controls of protecting data through its lifecycle.

The adoption and implementation of this policy is the full responsibility of the organization. NCSA does not take any responsibility for any damages related to un-informed decision of adopting and implementing this policy or out of the scope of this policy.

This policy has been developed based on the responsibilities assigned to NCSA as per Amiri Decree No.1 for 2021. 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.

TABLE OF CONTENTS

1. Introduction

The digital transformation and technical revolution have a significant impact in all fields. A clear reflection of this impact are the various services offered by organizations, most of of which have now become digital. Data is the focus in this revolution. This has been obvious with observing the huge amount of data, that is generated and how organizations have harnessed modern technologies such as Big Data technologies, Machine Learning and Artificial Intelligence, to not only deal with data but also yield enhanced value out of it.

One of the most important concepts is dealing with data in a clear, systematic, and easy-to-adopt methodology. Therefore, the need for data management is the cornerstone that organizations must implement by having a comprehensive overview and establishing the foundations for managing data in a business environment. Data Management, if achieved can result in many benefits, for example, but not limited to:

- Maintain competitive advantages in the market
- Provide assurance to customers and stakeholders
- Resource Management by optimizing available resources
- Achieve compliance with regulatory requirements.

Data has become a vital asset for organizations, which are exposed to many threats and often put them at risk. The following chart shows the most important risks and threats to the data, categorized by type of threats:

- Unauthorized disclosure of information
- Unauthorized modification of information
- Unavailability of information
- Regulatory Violations.

> From a national perspective, risks and threats could have impacts on national cyber security and economic stability.

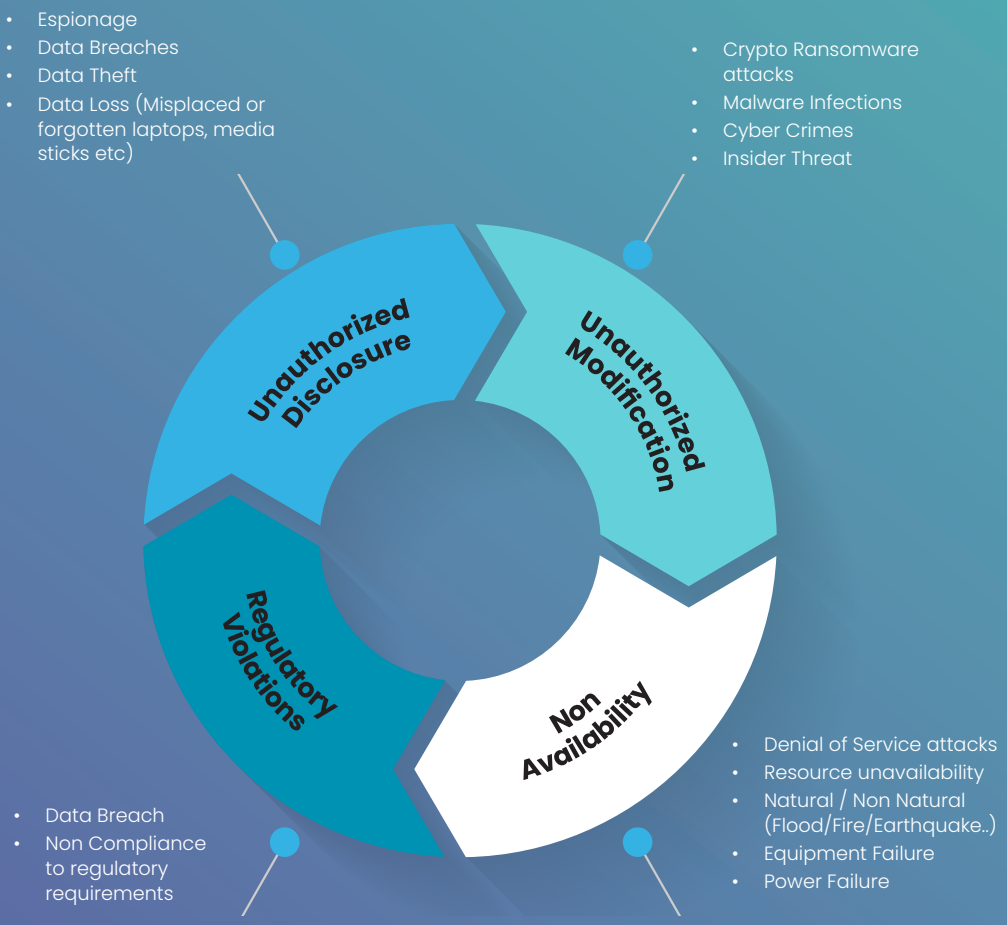

Figure 1: Risks and Threats to Data

It is important to understand that not all data is of equal importance or criticality, and that it is the role of organizations to understand this and classify the data, to optimally deal with it and protect data as necessary.

It cannot be hidden that without the use of a unified system and methodology for classifying data, all organizations will have different levels of asset protection, with no defined interpretations, which may hinder the business flow especially since data is mobile in nature.

2. Purpose, Scope, and Usage

2.1. Purpose

This policy aims to govern data classification on a national level and provide a national reference for the main principles in data management throughout its life cycle. It aims to protect the information and assets contained in data from potential risks and to facilitate the safe and accessible exchange of data while promoting interoperability

It also aims to unify the definition of data classification and create a consistent concept between authorities and organizations throughout the country. Additionally, it aims to establish a methodology to facilitate the adoption and implementation of projects and initiatives at the organizational or national level. Furthermore, the policy aims to guide stakeholders and help them understand the basic principles of data classification and labeling. This will enable them to apply these principles within their organizations in compliance with national policies.

2.2. Scope

This policy is applicable to all organizations and sectors in the State of Qatar, that are governed by the supervisory authority granted to National Cyber Security Agency (NCSA) in Amiri Decree No.1 for 2021 and in coordination with sector regulator in which the organization reports to.

2.3. Usage

This policy sets out a high-level methodology for classifying data for organizations in the State of Qatar. The rationale for classifying data into categories is to give appropriate values or degrees to the data and to identify its risks and appropriate protection methods to be followed for each category.

Consistent use of a data classification approach will streamline business activities within the organization, ensure adherence to accepted best practices when processing and protecting it, and help you get better returns on your security investment.

This policy is the cornerstone of National Information Assurance Standard and other national policies, standards and guidelines and cannot be dealt with separately. The National Information Assurance Standard is the complementary document to this document, which clarifies the main controls that organizations must take after they classify the data, which is updated according to the Procedures Fellowed.

3. Key Definitions

Data	Data is a fact or set of facts that have not been processed, i.e. in their original raw form or in an unstructured form.
Data Classification	Process of categorizing the data based on its security attributes (confidentiality, integrity, and availability), in order to handle it according to its security rating.
Data Classification Program	The activity that the organization will conduct to categorize and classify data based on the recommended methodology with the involvement of all relevant stakeholder
Government Organization	Organizations that report either to the Emiri Diwan, or the Prime Minister's Office, or the Council of Ministers.
Information	The data that has been processed and that becomes meaningful.
Methodology	Collection of methods, practices, processes, techniques, procedures, and rules to achieve a certain objective
Organizations	Refers to businesses operating within the State of Qatar.
Personal Data	Data of an individual whose identity is defined or can be reasonably defined whether through such Personal Data or through the combination of such data with any other data.

4. Data Classification Principles

This policy is based on the following set of core principles that must be considered when classifying data:

Principle 1: Understanding the nature of data

Understanding data is the starting point in the methodology used to classify data. It is important to understand data as it may have a bearing on the way it is handled, stored, secured, processed, or exchanged. We need to understand, if the data is structured or unstructured, what is the source of data, is the data personal or owned by an organization, does it contain in its nature, any kind of risk when it is collected or processed or shared, etc.

Principle 2: The lifecycle approach

Data, in its nature is changing. Therefore, classification may change during its lifecycle. Data could be at many different stages such as: creation, import, movement, modification, use, copying, storage, erasure or removal, restoration. Therefore, the process of classifying data must consider data lifecycle. The stages of data management lifecycle are addressed in the next section of this document.

Principle 3: Classifying based on risk assessment

The primary purpose of the data classification process is to take an approach that makes it easier for organizations to protect them from potential risks. Therefore, risk assessment is one of the basic principles that must be considered when classifying data, which determines the sensitivity and importance of this data for the work carried out by the organization. There are various schools of thought and methodologies in the market regarding how to assess risks.

Principle 4: Balancing Needs

It is important to consider the balance and proportionality between the risks that threaten the data, and the level of classification that is chosen. The data classification process must achieve the most appropriate classification level which is as low as possible but as high as necessary, along with the necessary level of protection without exaggeration and without adding any administrative, financial, or technical burdens that may constitute an obstacle to the conduct of business within the organization.

Principle 5: Establishing Data Governance

To ensure the success of Data Classification within the organization, it is important that the business establishes a suitable governance framework. It is recommended that a person within the management owns the data classification program and is accountable for its implementation and adoption within the organization. The process of classifying data does not belong to a single person or entity, but rather requires concerted efforts within the organization to ensure that the process is implemented in accordance with the principles and best practices. A high-level governance must be established across the organization with clearly defined roles and responsibilities for the different stakeholders within the organization.

5. Data Management Lifecycle

One of the main principles of the data classification policy is to integrate it within the data life cycle approach. The value of the data is not fixed, as its value may change according to the stage in which it is located, which is reflected in the degree of its classification. In some stages, they are of high value and sometimes they may lose their value completely, which leads to the need to decommission data.

The most important stages of the data life cycle:

1. Data Discovery
2. Data Classification
3. Data Protection
4. Data Reassessment
5. Data Decommission

The journey begins with data discovery, where we identify the sources of data, and inventory them, data is then classified based on its value and the principle of risk analysis and labelled accordingly, then based on the security rating of data, suitable controls for data protection are identified and implemented. The data life cycle approach emphasizes on the importance of reviewing and re-evaluating the data, which in turn will be reflected on the classification and controls. If data needs to be removed or destroyed, this needs to be done as per the data disposal procedures.

The Data Management Life Cycle is further discussed in details in Appendix A

6. Data Classification Scheme

6.1 Classification Scheme

Data is classified based on its importance and sensitivity, and this process is mostly done during the second stage of data management. Data is classified based on three basic criteria: Confidentiality, Integrity, and Availability.

This classification is done through the principle of risk analysis, which looks at the impact of the value of this data within the core business and objectives of the organization or business. It also considers the potential risks to the confidentiality, integrity, and availability of this data, and therefore a consistent classification is made with it.

Data is categorized based on the three criteria of: Confidentiality (denoted by the letter C), Integrity (denoted by the letter I) and Availability (denoted by the letter A). Starting with level (zero) which is the lowest impact and ending with level (3) which is the highest impact.

Using the following matrix, the three determinants and their levels are considered and dropped into the following matrix to identify their classification level as: High (denoted by the letter H), Medium (denoted by the letter M) or Low (denoted by the letter L)

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

Table. 1: Data Classification Martix

Rating levels (high, medium, low) are used on the organization›s assets, and the security controls needed to protect those assets are determined through various technical and administrative means.

6.2 Classification Labels

As a general best practice, labels are added to some assets in view of their classification, which makes it easier for the user to know how to deal with the data or information contained in those assets, especially if these assets are documents.

The data classification labels are linked to the classification of its confidentiality, to facilitate the knowledge of the required degree of protection or the flexibility available for sharing this data or information between the surrounding parties and using appropriate technological means.

The data classification labels parallel to the classification and specified in this policy are as follows:

▸ **C0**	Public
▸ **C1**	Internal
▸ **C2**	Restricted
▸ **C3**	Secret
▸ **C4**	Top Secret

The specified labels are mandatory for the government organizations. For non-government organizations, some flexibility may be permitted in the choice of labels such as for C3 levels, "Confidential" could be used instead of "secret", but it is necessary that the organization maintains one unified label scheme in its classification process.

Administrative and technical tools that enable the use of labels must also be provided including color-coding of label. wherever possible.

Below is an example of data confidentiality levels and their projection of labels, with some examples of intended audience.

Data Labelling Schema				
C0	**C1**	**C2**	**C3**	**C4**
Data that may be freely disclosed to the public	Data for Internal Use	Sensitive Data if compromised could negatively affect operations	Highly sensitive corporate or customer Data, that if compromised could put the organization at financial or legal or reputation risk.	Highly sensitive Top Secrets and Sensitive information
Intended Audience: Public	Intended Audience: Organization Users	Intended Audience: Defined users, roles or groups based on specific business rules	Intended Audience: Highly defined small set of users	Intended Audience: For your Eyes Only

Figure. 2: Data Classification Labels Scheme

However, the protection of the associated assets shall also be considered through their rating levels (high, medium, low).

7. Data Classification Controls

Depending on the level of classification that is selected, security controls that help protect data are selected and applied. Security controls are implemented in accordance with applicable national standards and guidelines. The National Information Assurance Standards is the standard adopted in the State of Qatar, with applicable national standards and guidelines issued by the National Cyber Security Agency (NCSA).

In addition to implementing security data classification controls, there are a number of important points to consider:

1. Each organization shall create its own internal Data Classification policy that is committed to following the data classification approach, in line with legislations in the State of Qatar, such as Personal Data Privacy Protection Law (Law No.13 for 2016), and Right to Access Information Law (Law No. 9 for 2022), as well as the national policies and standards.

2. The selected controls must be subject to the state of the data, as it may be either data-in-transit, data-in-use, or data-at-rest.

3. It is very important to consider the following steps while classifying data because of its great importance in ensuring the success and efficiency of the data classification process:

    - **Administration support:** requesting support from the highest administrative authority in the organization (the minister, the chief executive, and others).
    - **Collective agreement:** creating working groups or committees from several departments in the organization to implement the initiative, and defining roles and responsibilities
    - **Frameworks:** Define and implement the necessary policies and procedures for data classification and how to implement and review the process.
    - **Training and Awareness:** Promoting awareness and training the organization,s employees. All users must be aware of the tasks and duties related to data management. Therefore, the organization must provide the required training to employees about the classification method used in the organization and follow up on compliance with it.
    - **Technical solutions:** Identifying and implementing the available and appropriate technical solutions for the organization in this regard. The organization must provide technical solutions to facilitate the process of data classification, including data inventory, classification tools, adding tags, the method of sharing and processing it through its various stages in proportion to the required level of protection.

4. Clarity in roles and responsibilities: Defining roles and responsibilities about data classification and how to protect it is one of the most important determinants in reaching the goals related to the successful and efficient data management process.

5. The classification must be viewed in a balanced manner that achieves the required level of protection without overdoing it. The tendency to exaggerate the classification of data, will create a lot of obstacles at the administrative and physical level.

6. C1 is the default classification for unclassified data which corresponds to the label: (internal).

7. In the case of dealing with personal data, which is data about an individual whose identity is reasonably determined or can be managed, it is important to mention that this type of data is subject to the Personal Data Privacy Protection Law (Law No. 13 of 2016) and the policies and guidelines

issued by the competent department of the National Cyber Security Agency (National Office for the Protection of Personal Data Privacy). Within the context of data classification, it is recommended to classify and label Personal Data with Restricted C2 and Sensitive Personal Data as Secret C3, in view of the parties responsible for managing personal data and the required purpose of processing this data. These recommended classification labels shall not be used as default and it should be subject to apply the recommended data classification methodology

8. Roles and Responsibilities

The data classification management process is an integrated process that includes several stages (see Annex 1 on the stages of data management), so it is necessary to define roles and responsibilities during these stages.

The governance of data management is a key success factor to achieve optimum results where all relevant stakeholders know their roles and responsibilities, in addition to establishing accountability. Designing governance model in organizations has different factors dependent on the organization's nature, organizational structure, and other factors. However, among the most important roles and responsibilities that could be in any organization are the following:

Chief Data Officer: The person assigned by the senior management to be accountable for the Data Classification Program in the organization. He will be responsible for developing the necessary policies and procedures to manage data and its classification as well as observing the appropriate controls to secure the data. He will also be responsible for assigning and overseeing the roles and responsibilities to different stakeholders for an effective Data Classification implementation in the organization.

Data Owner: The person responsible for the data owned by the organization, and he is the one who has the right to make decisions in determining the value of the data in view of the business process in the organization. The data owner is often responsible for the business unit of the organization, and therefore has sufficient knowledge of the value of the data and can make decisions at the level of its classification. The data owner is also responsible for ensuring and naming records for data classification when they are created and can assign these tasks to (Data Classification Specialist).

Data Custodian: The person responsible for protecting data by making the decision to use security controls commensurate with the classification, and this person is often from the Information Technology Department, who has the technical expertise and the necessary knowledge of the best practices used in the application of security controls and data protection at its various stages in accordance with the policies and standards adopted.

Data Consumer or User: is the person who deals with, uses and processes data according to the workflow entrusted to him, and he must be knowledgeable, sufficiently informed, and responsible for adhering to the optimal way to use and protect data according to the policies followed in the organization and to abide by the tasks entrusted to him during the stages of data management data and not expose it to potential risks.

Data Classification Specialist: A trained person who has the ability to understand business data and is assigned the task of assisting the various departments in the organization to provide data classification support in line with the organization›s strategy and policy. It is often someone from the same business unit as the data owner, so they have the ability to understand, value, and categorize business data.

Data Auditor: The person responsible for reviewing the classification of data and determining whether it is in line with business, regulatory, compliance and other requirements. It also looks at security controls and technological solutions provided for their application and consideration for their development and improvement. The data auditor also reviews suggestions from data users and assesses the alignment between actual data use and existing data processing policies and procedures. It is likely that this person belongs to the administrative units of corporate governance and quality management.

9. Policy Clauses

Through this policy, the National Cyber Security Agency defines the national data classification scheme to be used within the State of Qatar. This section 9, within the policy will be deemed as the Normative section for any compliance related queries.

1. The policy defines five (5) levels of classification shall be used for government entities in Qatar. Non-government entities shall use a minimum of four (4) levels of classification.
2. In line with the classification levels, the organizations shall use a corresponding Data Classification Labels. These are C0 - Public, C1 – Internal, C2 – Restricted, C3 – Secret, C4 – Top Secret.
3. The default classification label for unclassified data shall be C1 – Internal.
4. The data shall be secured and protected based on the security classification covering Confidentiality, Integrity, and Availability.
5. The data classification principles defined within this policy (Section 4) shall be used as the guiding force to arrive at the appropriate classification level for the data.
6. The organizations shall manage their data throughout the data life cycle and ensure that suitable processes are implemented to facilitate the same.
7. In line with this policy, each organization shall issue its own policy mandating the Data Classification Scheme provided in this policy.
8. Each organization will assigned a person who will execute the responsibilities of the "Chief Data Officer" and will be accountable for managing the governance and the program for Data Classification.
9. The "Chief Data Officer" shall ensure that the Data Classification Program:

a. Is supported and has the necessary commitment from management.

b. Aligns the expectations of the business stakeholders regarding the security of the data

c. Is focused on creating the necessary awareness and imparting the relevant skills to the different users in the ecosystem about data classification

d. Evaluates the necessary technology to facilitate the adoption, user satisfaction, and success of the program.

e. Implements the required governance for execution of the program and clearly communicates the necessary roles and responsibilities within the organization.

10. The "Chief Data Officer" can communicate the challenges, if any about the Data Classification program with the competent department within the NCSA.
11. The National Cyber Governance and Assurance affairs shall be the competent department for administrating this policy within the NCSA.

10. Compliance and Enforcement

10.1. Compliance and Enforcement

The policy lays the foundation for implementing an Information Security Management System within and organization and will be complemented by the National Information Standard V2.1 which identifies the relevant security controls that organizations need to implement based on the security rating of the data.

10.2. Transitioning and effective date

10.2.1. Effective date

The policy will be effective upon publication on NCSA official channels.

10.2.2. Transition period

Organizations impacted by this policy will be provided a window of six (6) months effective the date of publication, to demonstrate their roadmap to comply with this policy.

10.3. Exceptions and deviations

The policy mandates that organizations within the scope of this policy, classify their data based on the data classification scheme.

Any other deviations to this policy shall be communicated to the National Cyber Security Agency by the organization, through an official correspondence explaining the justifications and rational, along with a risk management plan identifying the risks, assessment of the risk, mitigating controls, and communication and acceptance of the risk by senior management. Based on this, the NCSA will provide an assessment of the exception request in coordination with sector regulator (where applicable).

APPENDIX A

Data Management Lifecycle

The life cycle of data is not fixed, as the value of data can change over time and sometimes it can lose its value completely, leading to the need to decommission (or disposing) it.

The main stages of the life cycle of data:

▸ 1.	**Data Discovery**
▸ 2.	**Data Classification**
▸ 3.	**Data Protection**
▸ 4.	**Data Reassessment**
▸ 5.	**Data Decommission**

1. **DATA** DISCOVERY

Data Discovery consists of two steps:

1. Discover where does the Data come from, the data sources and
2. Creating an inventory of the Data

Discover Data Source:

To understand the sources of your data, you need to know your business processes, services, and functions. You also need to understand the data flows within those business processes, services, and functions. What data sets are used as inputs, what processing is performed and what data is produced as output for each of these processes, services, and functions.

You also need to know where all your data is located, stored, and processed. Primarily, data is generated in one of the following three ways:

Data Creation:

This is creation of records/data from scratch.

Examples: Creating a new document in a word processing application, writing a new email, creating an event log by a system, etc.

Data Processing:

This is the processing of existing records by an application or a system to create a new record/data.

Examples:

Creation of a monthly attendance report or payroll based on daily attendance data, response to an incoming email, an alert created by a SIEM solution based on event logs, etc.

Data Import:

This is the import of data from an external data source (media and/or system). Example: Importing files from a USB stick, machines sending logs to a central syslog/SIEM server, records from an attendance system sent to the payroll system etc.

Data Inventory:

This is a formal process of inventorying various records you have in your organization.

As with any other inventory, the process needs to capture the ownership of the data assets, including the associated processes and systems.

2. **DATA** CLASSIFICATION

Assign a data classification based on the criticality and sensitivity of the data, based on the approved classification scheme. Label the data based on the assigned confidentiality classification.

3. **DATA** PROTECTION

Depending on the criticality and sensitivity of your data, you need to implement appropriate controls to protect the confidentiality, integrity, and availability of your data. The controls you choose will also depend on the state of the data in terms of Data in Transit, Data in Rest and Data in Use. NIAS suggests baseline controls for all datasets. Datasets classified as M or H require additional controls that correspond to the attributes (C or I or A) that led to the classification of the dataset as M or H. Data classification provides you with this transparency and understanding and helps you allocate your resources (time, effort, and manpower) accordingly to ensure an optimal return on your security investment (ROSI).

4. **DATA** REASSESSMENT

The value of data may change from time to time based on various factors such as processing cycle, time, right of use, applicability to business, etc. This in turn can affect the classification of data. From time to time, businesses (users) need to assess and validate the classification of data. Such assessments are carried out at least annually and/or at the end of the specified data retention period. Based on this reassessment, corrective action must be taken on the controls applied.

5. **DATA** DECOMMISSIONING

Data is normally disposed of for one of the two reasons:

a. End of data life cycle: it is not advisable to keep data forever. Once data has served its purpose, it must be decommissioned and deleted from systems to end its life cycle. Agencies should consult with their legal department and establish data retention policies within their organization. All legal requirements, business requirements, contractual requirements and other should be considered when determining the retention period for data.

b. Legal requirements: You may have a legally binding reason to delete data from your systems. This could be the case if there is a:

   1. User requests: under data protection laws such as Qatar PDPPL and GDPR, users may request organizations to delete their personal data from their systems.

   2. Takedown requests: the organization may knowingly or unknowingly have illegal, unlicensed or proprietary information on their systems that may constitute a breach of the law. If such information is identified, it must be removed with immediate effect.

Organizations must also consider whether it is necessary to obtain permission before releasing data and, if so, implement appropriate controls.

Lastly, users must be educated about and use safe disposal methods depending on the classification of the data.

APPENDIX B-

General Approach For Program Implementation

The Data Classification Policy will be applicable and implemented across the organization. And although certain steps shall be implemented at the onset across the organization, when it comes to technical implementation of controls you may feel the need to break the technical implementation in defined sub scopes. The following is a high-level approach that can be used as a guidance by organizations to design and implement a Data Classification program within their organization.

Step 1: Management commitment: Management must formally introduce the data classification program in their organization.

Step 2: Management must appoint a person as ‹Chief Data Officer› who has the appropriate skills and business understanding to lead and manage the program.

Step 3: Management must allocate the necessary resources (funds, staff) to the program.

Step 4: The «Chief Data Officer» sets the roadmap for implementing a data classification program within the organization in accordance with this policy.

Step 5: The Chief Data Officer will establish the governance required to implement this program. This will include, but not be limited to, the necessary policies, procedures and assignment of roles and responsibilities.

Step 6: The Chief Data Officer will establish an awareness and capacity building program within the organization.

Step 7: The ‹Chief Data Officer› will evaluate appropriate technologies to facilitate the implementation of the data classification policy within the organization.

Step 8: Depending on the size of the organization/company, the technical implementation can be divided into different areas to facilitate execution.

Step 9: It is important that the implementation focuses on your critical processes and functions. Therefore, organizations should conduct a Business Impact Analysis (BIA) to identify the critical processes/functions in the organization. These critical processes/functions should be prioritized over other unimportant business processes.

Step 10: Define the scope of the program.

Step 11: Within the defined scope, identify the relevant data assets and create an inventory of the assets through a data discovery process. OBASHI is one of the methods that can assist you in this task.

Step 12: Perform data classification for the identified data assets. This will help you understand the overall criticality of the data and the appropriate data classification label.

Step 13: Deploy the necessary technology to facilitate the classification labels of the data.

Step 14: Consider the overall security requirements for the data and implement the necessary controls based on the National Information Assurance Standard V2.1.

Step 15: Implement processes to re-evaluate data classification and re-evaluate data from time to time based on relevant business triggers.

APPENDIX C-

Business Impact Analysis (Bia) Methodology

To determine the priority for classification of information assets, a weighted impact assessment needs to be undertaken. If the Agency has an existing method for assessment of business impact, this lowercase to may be used instead of the one provided in this Appendix.

It is recommended that BIA is undertaken by rating the impact of loss or degradation of a process/service/function on the Agency using the following impact factors:

1. Impact on Reputation
2. External Impact (impact on external entities, other Agencies, public etc.)
3. Internal Impact (impact on employees and the Agency itself)
4. Legal Impact (liabilities due to non-fulfilment of legal obligations e.g. not complying with service level agreements, regulations, legislation etc.)
5. Economic Impact (loss of direct revenue, lost opportunities etc). The following steps should be undertaken to rate a processes criticality:

1. For each of the impact factors, rate the factor's importance to the Agency, based on the following rating. This weighting factor (a1 to a5) is calculated only once and is used for each process being assessed. The "a" is the management's perspective of the impact.

- **0** No impact
- **1** Low impact
- **2** Medium impact
- **3** High impact
- **4** Very high impact

2. For each process, identify the impact (I) to the Agency upon its loss or degradation, using the following scale. For time dependent processes, ensure that impact at peak usage times is calculated. The weighing factor "I1 to I5" is the process/service/function owner's perspective of the impact.

- **0** Not Important
- **1** Low importance
- **2** Medium importance
- **3** High importance
- **4** Very high importance

3. Use the following formula to determine a criticality (on a scale of 100) for each process. : impact value =1.25 (a1I1 +a2I2 +a3I3 +a4 I4 +a5I5)

Worked Example

Organizational Impact Factor weightings:

- **1.** Reputation Impact Weight: High importance (a1=3)
- **2.** External Impact Weight: High importance (a2=3)
- **3.** Internal Impact Weight: Medium importance (a3=2)
- **4.** Legal Impact Weight: Very high importance (a4=4)
- **5.** Economic Impact Weight: Medium importance (a5=2)

Process Name: Salary Processing, Impact at Critical Time

- **1.** Reputation Impact: High impact (I1=3)
- **2.** External Impact: Low impact (I2=1)
- **3.** Internal Impact: High impact (I3=3)
- **4.** Legal Impact: Low impact (I4=1)
- **5.** Economic Impact: No impact (I5=1)

Impact value = 1.25 (3x3 + 3x1 + 2x3 + 4x1 +2x1) This would yield an impact value of: 30.

www.ncsa.gov.qa

Tel: 16555 | Fax: 2362080

Email: info@ncsa.gov.qa | P.O. Box: 24100 Doha - Qatar

Follow us: