Data Classification Policy

State of Kuwait

v 2.3

Communication and Information Technology Regulatory Authority

(CITRA)

Contents

1. Terms and Definitions:

The following terms and expressions, wherever mentioned in this document, shall have the meanings assigned to them below. The definitions mentioned in the Communication and Information Technology Regulatory Authority Law No. 37 of 2014 and as amended by Law No. 98 of 2015, its executive regulations, and the ICT Terms and Definitions document.

Term	Definition
1.1 Data	It is information that is edited, modified, printed, or stored by means of a computer, and this information is in the form of text, audio, pictures, or video files, or in the form of computer programs or digital information in a language that the computer understands.
1.2 Personal Data	It includes information or a set of information, if collected, the identity of the individual can be clearly and directly inferred. It also includes any information that can be linked indirectly, like the location data for a specific person, regardless of whether the identity of the individual is clear or not from that information or from a combination of data from that information.
1.3 Data Classification	It is the classification (or placement or arrangement) of data in appropriate security levels based on their sensitivity to determine the best means to use, share, and protect them.
1.4 Data Owner	It may be an individual, government entity or one of its sectors, or a private company or one of its sectors, where he owns certain data and has the authority to process, amend, copy or store it (for example, the human resources sector owns the data of the entity's employees, the information technology sector owns the infrastructure and applications data, the finance department owns the salary data, the customer care department owns the customers data, the procurement department owns the purchase data, etc.).
1.5 Encryption	The process of converting data from readable text to unreadable text, where the encryption process is applied both during data storage and when transferred over networks.
1.6 Data Breach	Any loss of data, misuse or disarrangement, access, and modification to data by unauthorized persons, or disclosure to unauthorized persons.

2. Introduction

This policy outlines a methodology for data classification for the public and private sectors. Which, when followed, leads to defining the acceptable level of security protection, ensuring adherence to acceptable best practices, and determining the means for data handling, transmission, and processing. Whereas the failure to follow any approach to classify data and provide the necessary protection for each category would expose this data to various electronic risks such as data leakage, wrong handling and sharing, or penetration.

2.1 Data Classification Objectives

2.1.1 Objective: classifying data into separate categories helps in better decisions making, regarding data access and processing in line with the data classification levels mentioned in this policy, which contributes in helping the government or private entities to take all necessary measures to enhance the security and protection of their data and the personal data they have of the individuals, in a consistent manner with the requirements and institutions plans, laws and regulations applicable in the State of Kuwait.

2.1.2 Scope: the policy scope includes data that is processed, stored, modified, or transferred by computer or smart devices, i.e., digital data (structured or unstructured), which government and private entities create, collect, and maintain as part of their official business functions and use or share for the purpose of providing public services. Examples of structured data include individuals' data (such as personal or company data), non-customer data (such as environmental data), and organizational data (such as human resources, finance, and data related to assets and purchases). Unstructured data includes text-based data (but not limited to word processor documents, presentation slides, photos, video clips, and audio recordings), data of printed documents fall out of the scope of this policy. As for the access of printing or copying digital data, they must be determined based on the sensitivity of the content and according to the level of classification in which they fall under.

3. Data Classification Policy

3.1 Policy Items

3.1.1 The data owner shall classify their data into at least four levels. Entities of a security or military nature of the country are excluded from adherence to the classification levels specified in this policy, and they have the option to classify their data as they see appropriate. If the data owner has a different classification system, mapping must be made to the classified data with the classification system mentioned in this policy.

3.1.2 The owner of the data is free to choose their data protection methods according to their data classification, retention, collection, and processing schemes. The data owner must

also ensure that necessary protection is provided to their data storing scheme depending on its classification, especially Tier 3 and Tier 4 data, to protect them from hacking.

3.1.3 The data owner is required to create and maintain a data catalog which should include the metadata information and standards for its data in a unified format. This catalog should also be updated periodically.

3.1.4 The data owner must encrypt all classified data that falls under Tier 3 and Tier 4 during transmission from one government entity to another, or when transmitted between different physical geographical locations of government entities; this applies to the private sector as well.

3.1.5 The data owner must ensure that all data classified according to the third and fourth levels are transferred or removed from data centers and servers before the disposition of the equipment of data centers and servers hosting the data.

3.1.6 The data classification levels mentioned in this policy have been developed based on the best regional and global practices, and the data owner is free to use other classification levels if they are best suitable with the type of data they have, in accordance with international best practices and standards such as NIST 800-53, NIST SP 800-60, ISO 27001, PCI DSS, and HIPAA to ensure the validity and quality of classification.

3.2 What to consider before starting the data classification process

3.2.1 Data gathering, auditing, and analyzing processes. Incomplete, vague, or ambiguous data should be excluded or modified.

3.2.2 Considering the accuracy in sorting and placing data in the classification levels in accordance with this policy, to determine and evaluate the risks on each level to ensure the safety and protection of the data.

3.2.3 Forming a data classification team headed by the senior management or their representatives, with the membership of the Director of Information Security, the Director of the Information Technology Department, in addition to the directors of the various departments that own or store the data of the entity, whether this data is personal and belong to subscribers or data belonging to the entity itself. As this team is responsible of classifying the data in the entity and labeling it according to its sensitivity level and in line with what is stated in this policy.

3.2.4 In order to ensure the full implementation of data classification and to support the unification of procedures between the various entities, the authorities must do what is necessary towards developing a road map and an action plan that explains how to implement the process of classifying data according to the four basic levels described in this policy, provided that the data classifications is to be reviewed internally in an appropriate periodic and fixed manner.

3.2.5 Determine and prioritize data sets, classify the data of high priority before other groups of lower levels of priority, where priority level is according to the importance of the data,

its sensitivity and business value. This depends on the current data management maturity level within the entity, the size of the entity's operations, and the extent of data importance to its functions.

3.2.6 Government and private sector entities shall be responsible for defining the roles and responsibilities of the of its workforce, to implement the data classification policy within its scope.

3.2.7 The roles and responsibilities for managing and classifying the data are determined according to the discretion of each entity as it deems appropriate, as each entity differs from the others in terms of infrastructure and procedures for managing the data. The entity can decide to create new jobs to fulfill these roles or add responsibilities to the current roles.

3.2.8 The sensitivity of the data should not be overemphasized.

3.3 Data Classification Tiers

Tier	**Description**
The First Tier: "Public Data"	Refers to unclassified data available to the public or data that is not protected from public access under any law, regulation, or contract and does not require any encryption, as it does not indicate the owner of the data or has the impression of the government or private sector data. Some examples include: 1. Open data such as policies, regulations and laws published on websites, daily newspapers, magazines, or other publications. 2. Self-service forms available to individuals and institutions. 3. General data and information publicly available on websites.

The Second Tier: "Private Insensitive Data"	Refers to data owned by the public and private sectors or at a personal level. It is data that indicates insensitive private data that indicates the identity of the data owner, and unauthorized disclosure does not lead to any damage to the privacy of the data owner. Examples include, but are not limited to: 1. First or last name 2. Job title, job duties and employer name 3. E-mail address 4. Civil ID number 5. Gender 6. Age 7. Academic qualification 8. Social status 9. Contact data such as: work phone number, mobile phone number, or home phone number 10. Address
The Third Tier: "Private Sensitive Data"	Refers to data owned by the public and private sector or at a personal level. It is data indicating the identity of the data owner, and related to the content of the data owner, and may include part of the insensitive data, and unauthorized disclosure leads to damage to the privacy of the data owner. Examples include, but are not limited to: 1. Minutes of meeting and business plans 2. Internal project reports 3. The files of the lawsuits and the preliminary and final provisions issued therein, the decisions and orders of the courts and all related files 4. Legal notes and opinions issued by legal offices 5. Medical records 6. Criminal fingerprint and DNA fingerprint
The Fourth Tier: "Highly Sensitive Data"	Refers to private data of a very sensitive nature, and the unauthorized disclosure of this data may inflict great damage on the privacy of the owner of the data. Or those data owned by the government or private sector entities or at personal level of individuals or at the national level, and therefore it should be published to a very specific segment of those who need access to it. This data must have high encryption requirements and requires the highest levels of protection and security. Some examples include, not limited to: 1. Encryption keys 2. Political documents, international negotiations, or international relations data 3. Sensitive information of military nature or related to the state security

3.4 Roles and Responsibilities

3.4.1 Roles and responsibilities of public and private sector entities who own their data or individuals' data

All public and private sector entities must take the following into consideration when classifying their data and the personal data of individuals they have.

Levels	Description
Top Management	1. Circulate this policy to the entity's employees in its various sectors and ensure that they understand its content and process the entity's data in line with this policy. 2. The entity or company must form a data classification team headed by the senior management or their representatives, with the membership of each of the director of information security department, the director of the information technology department, in addition to the directors of the various departments who own data, whether the data is personal and pertains to subscribers or it is the entity or company data. As this team classifies the data in the entity and label it according to its sensitivity level in line with what is stated in this policy. 3. Directing the entity's employees to immediately report any breach in the implementation of this policy. 4. Record breaches and take corrective actions. 5. Approving the classification provided by the data owner in the entity. 6. Monitor and confirm the entities' compliance with what is stated in this policy and the Data Classification and Handling Procedure Guide if issued by the Communication and Information Technology Regulatory Authority (CITRA). 7. Assign a focal point employee to communicate and provide the Central Agency for Information Technology (CAIT) with quarterly reports on the extent of implementation of this policy, as CAIT is the supervisor of the implementation of the regulations and policies issued by CITRA.
Data Owner	1. Participate with the data classification team mentioned above in classifying the owned data according to what is stated in this policy. 2. Identify the risks related to the data, determine the best ways for protection, and take the necessary support from the entity's information technology department to provide a safe environment for hosting the data. 3. Make periodic reviews and evaluations of the classified data and amend it if necessary.

Information Technology Department	1. Supporting the entity to implement the policy by providing technologies that enable data owners at the entity to classify their data. 2. Provide the appropriate infrastructure and security standards to enable classification and protection of data according to the requirements of classification tiers mentioned in article 3.3 of this policy.

3.4.2 Roles and responsibilities of the Communication and Information Technology Regulatory Authority (CITRA)

3.4.2.1 Issue policies and guidelines related to information and communication technology.

3.4.2.2 Monitor the public and private sectors entities in implementing the policies and guidelines issued by the authority to ensure compliance.

3.4.2.3 Request periodic reports from the Central Agency for Information and Technology (CAIT) to analyze and measure the compliance and implementation of government entities with this policy. Reports to contain the following:

- A catalog of all the data available and hosted at the entity, which must include metadata in a unified format.
- The documents that show the approved classification tiers followed by the entity with explanation of the bases and criteria used to set the classification tiers.
- The documents that clarify of the methods used for data protection and encryption in accordance with the classification system used when hosting, storing, and processing data.
- The documents that show the locations of stored data according to classification tiers.
- The roadmap for data classification process, with action plans and operations of the entity to ensure the accuracy and quality of the data classification.
- A periodical progress report on the extent of the achievement in accordance with action plans and in line with this policy.

3.4.2.4 Coordinate with the Central Agency for Information and Technology (CAIT) to develop an implementation plan within a period not exceeding three months from the execution date of the policy, to enable the implementation of the policy with the government entities. Provided that the conditions of government entities are to be reconciled in accordance with this policy within a period not exceeding two years.

3.4.2.5 Hold workshops and awareness sessions to increase the awareness level and help entities implement the policies and guidelines issued by the Communication and Information Technology Regulatory Authority (CITRA).