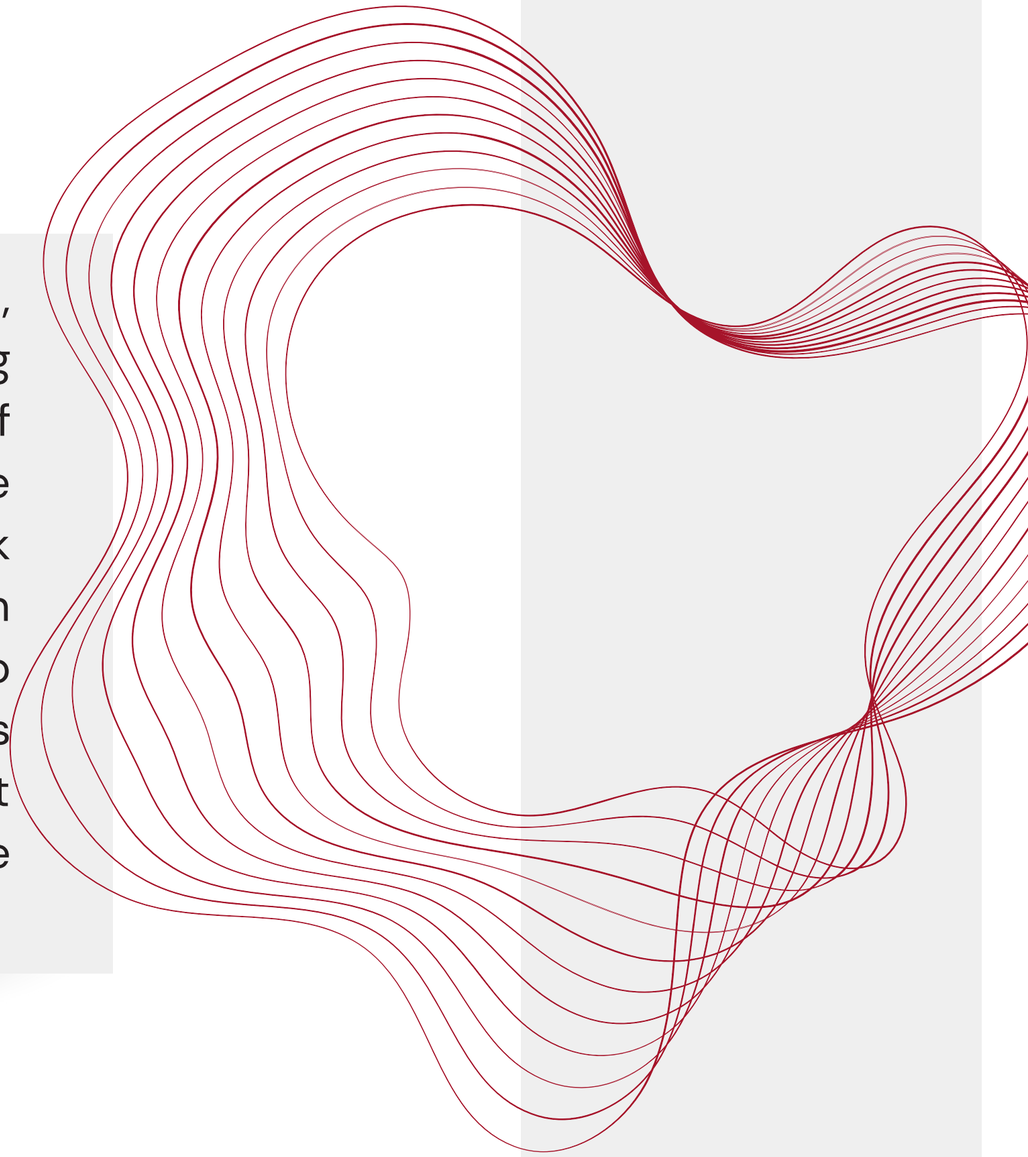
GLA
& CO

WWW.GLACO.COM

CONTENT

INTRODUCTION

On June 6, 2023, The National Cybersecurity Center, ("**Center**") took a significant step in safeguarding digital privacy with the issuance of Decision No. 7 of 2023 ("**Decision**"). This Decision pertains to the implementation of a comprehensive national framework aimed at classifying electronic data based on sensitivity and importance levels, and is applicable to civil, military, security governmental entities, as well as public and private sector institutions in Kuwait ("**State**"), which are related to the Center's scope ("**Relevant Entities**").



ABOUT THE CENTER

Decision No. 37 of 2022 was issued regarding the establishment of The National Cybersecurity Center.

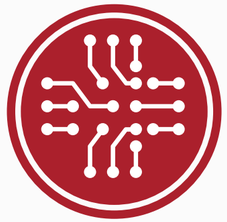
The Center aims to achieve the objectives derived from The National Strategy for Cybersecurity ("**Strategy**"), particularly the following:

1. Building an effective national cybersecurity system, developing and organizing it to protect the State from cyber threats, and efficiently and effectively confronting these threats in a way that ensures the sustainability of operations and the preservation of national cybersecurity.
2. Protecting vital interests in the electronic space, and supervising the development of specialized national capabilities in the field of cybersecurity.
3. Enhancing the cybersecurity culture that supports the secure and proper use of the electronic space.
4. Protecting and monitoring vital assets, infrastructure, national information, and the information network within the State.
5. Providing methods for cooperation, coordination, and exchange of information among various local and international entities in the field of cybersecurity.

SCOPE OF APPLICATION

This Decision applies to all electronic data that is created, stored, or processed by any employee or any third party contracted with.

KEY DEFINITIONS



ELECTRONIC DATA

The data with electronic characteristics in the form of texts, codes, sounds, videos, graphics, images, computer programs, or databases, which is created, received, processed, or stored electronically.

SENSITIVE DATA

The data for which access, viewing, processing, or sharing is restricted to specific individuals or entities. The loss, misuse, unauthorized access, or non-permitted disclosure of this data by any person or entity can lead to severe harm or negative impact on national security, public safety, state economy, or the privacy and health of individuals. It includes potential damage to persons, properties, intellectual property, operations of relevant entities, assets, or their individuals. Additionally, these data might be classified as sensitive according to the applicable laws in Kuwait or the judicial authorities.

RESTRICTED DATA

The data for which access, viewing, processing, or sharing is restricted to specific individuals or entities, and is not considered sensitive data.

PUBLIC DATA

The data that is available to everyone without restrictions, and anyone or any entity can access, view, process, or share them freely.

PUBLIC POLICY & RESPONSIBILITY

PUBLIC POLICY

1. The Relevant Entities are obliged to classify Electronic Data by determining the level of sensitivity and importance of their Electronic Data based on its nature. The Relevant Entities must also ratify it from the Center.

2. The Relevant Entities are obliged to classify Electronic Data according to its nature, level of sensitivity, impact, and importance into different categories and levels.

3. The Relevant Entities are obliged to take the necessary measures to issue a policy specifying the classification of their Electronic Data, which shall include details of the categories of classified Electronic Data.

4. The Relevant Entities are obliged to take the necessary technical and organizational measures to ensure appropriate protection and security for each category of Electronic Data, according to its classification.

5. The Relevant Entities are obliged to obtain the Center's approval before storing any sensitive data or processing it outside the state of Kuwait.

6. The Relevant Entities bear the responsibility of monitoring the classification of data by individuals when created or received from other entities. The classification is carried out within a limited time frame, and periodic updates of the classification are also conducted.

7. The Relevant Entities are obliged to provide appropriate training for their employees and personnel regarding the Electronic Data classification policy.

RESPONSIBILITY

- The Relevant Entities bear the responsibility of issuing their Electronic Data classification policy and ratifying it from the Center.

- The Center is responsible for reviewing and approving the draft policy of Electronic Data classification for the Relevant Entities.

- The Relevant Entities must conduct periodic evaluations of the effectiveness of the Electronic Data classification policy, ensuring its proper implementation, and continuously updating the classification. They should also submit regular reports to the Center regarding the results of the implementation and application of their Electronic Data classification policy.

- All employees working for the Relevant Entities are responsible for adhering to the policies and procedures related to the classification of Electronic Data applicable to their respective organizations.

- The Relevant Entities and their employees must report any suspicion, violation, or criminal activity related to Electronic Data to the competent authority within the Relevant Entities, in accordance with the laws, regulations, and rules applicable in the state of Kuwait. Such reporting is essential to maintain the confidentiality, integrity, security, and availability of Electronic Data.

GLA
& CO

WWW.GLACO.COM