CITRA

الهيئة العامة للاتصالات وتقنية المعلومات

COMMUNICATION & INFORMATION TECHNOLOGY REGULATORY AUTHORITY

Cloud Computing Regulatory Framework

State of Kuwait

V2.4

Communication and Information Technology Regulatory Authority

Index

Introduction

Cloud computing technology has become one of the most important technologies that are needed to succeed in a comprehensive digital transformation process, as the transition to the cloud offers many benefits that serve both the public and private sectors as well as individuals. In this context, the Communication, and Information Technology Regulatory Authority (CITRA) is keen to activate its supervisory and regulatory role according to its establishment law No. 37 of 2014, as amended by Law No. 98 of 2015, by setting up regulations to regulate the telecommunications and information technology sectors in line with the state's general policy to achieve comprehensive development. Based on that, the Cloud Computing Regulatory Framework was created to regulate the use of cloud computing services within the State of Kuwait. In addition to this framework the Communication and Information Technology Regulatory Authority (CITRA) has issued a set of mandatory and indicative policies and guides that support and comply with the provisions contained within this framework, and they are as follows:

1. Data Classification Policy
2. Cloud First Policy
3. Data Privacy Protection Regulation
4. Cloud Service Providers Regulations and Commitments
5. Subscribers Guide to Cloud Services
6. Cloud Migration Guide

All the clauses with the various articles mentioned in the chapters of this document are binding and obligatory to all parties concerned with using cloud computing services, unless otherwise stated.

Definitions

The following words and expressions wherever they may appear in this framework shall have the meanings assigned to them below, in addition to the definitions contained in the Communication and Information Technology Regulatory Authority Law No. 37/2014, as amended by Law No. 98 of 2015 with its implementing regulations, and in the list of ICT Terms and Definitions, the Data Classification Policy, and the Cloud First Policy issued by CITRA.

State: The State of Kuwait.

CITRA: Communication and Information Technology Regulatory Authority.

Framework: The Cloud Computing Regulatory Framework.

Cloud Computing: It is a model for enabling convenient and on-demand network access to a common set of configurable computing resources (for example: networks, servers, storage, applications, and services) that can be quickly provided and launched with minimal administrative effort or interaction from a cloud computing service provider.

Cloud computing services: Information and communication technology (ICT) products and solutions that use information systems resources and platform capabilities as needed at any

time, and through any network (fixed or mobile), and by any network-connected devices, and by means of the cloud. They are divided into three types of service:

- **Infrastructure as a Service (IaaS):** In this model, the service provider hosts the infrastructure components that make up a data center such as servers, storage, networking hardware, and a subscriber's virtualization layer. The subscriber does not manage or control the basic cloud infrastructure, but he controls the operating system, storage, applications, and some protection systems, including, but not limited to mainframe computers, storage, load balancers and virtual machines.
- **Platform as a Service (PaaS):** In this model, the service provider provides the environment that includes the hardware and software tools required to develop applications for subscribers via the Internet. The service provider hosts hardware and software on its own infrastructure and thus exempts subscribers from purchasing an infrastructure to install new ICT solutions, including but not limited to application development, databases, middleware, testing tools and developer tools.
- **Software as a Service (SaaS):** The software distribution model in which the service provider hosts the applications and makes them available to the subscriber via the Internet. These include, but are not limited to government applications, web services, virtual computers, customer relationship management (CRM) systems.

Cloud computing service provider (service provider): Any authorized person who provides one or more of the cloud computing services detailed above to subscribers of cloud computing services. They may own a center or data centers that they manage partially or completely which is used to provide these services, directly or indirectly, through a cloud computing services broker or through a cloud computing services aggregator.

Entity: It includes the ministries, departments, institutions, agencies, and independent subsidiaries and companies of the government of the State of Kuwait. Except for those entities of a security or military nature, where they have the option as they see fit.

Company: includes private companies and institutions owned by entrepreneurs and is not classified within the government sector entities.

Individual, individuals: Includes citizens and residents of the State of Kuwait.

Cloud computing subscriber (subscriber): An individual, government entity, or private company who uses cloud computing services by purchasing those services from a cloud computing service provider under the cloud computing contract.

Cloud computing user: Any individual who uses cloud computing services provided to a cloud computing subscriber according to the nature of the relationship between the user and the subscriber. This individual may be a user and a subscriber at the same time if the user concludes a cloud computing contract with a cloud computing service provider to benefit from those services on a personal level.

Cloud computing contract: It is a commercial agreement concluded between subscribers of cloud computing services and between a provider of cloud computing services to provide those services to them.

Service Level Agreement: It is a commitment between the cloud computing service provider and the subscriber, as this commitment includes several aspects: the quality of the services provided, the availability of services, and the responsibilities of the cloud computing service provider and the subscriber to the cloud computing services. This agreement also stipulates that the services provided by the cloud computing service provider to the subscriber are as agreed upon in the contract signed between the two parties, and the confidentiality of information and data between the two parties is guaranteed.

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, behavioral information, preferential information, or digital information in a language that the computer understands.

Personal data (Personally Identifiable Information (PII): Defined in the Data Classification Policy "which includes information or a group of information, if collected, through which it is possible to clearly and directly infer the identity of the individual. On any information that can be linked indirectly as location data for a specific person regardless of whether the identity of the individual is clear or not from that information or from a group of that information and other information, and as mentioned in the Cloud Computing Regulatory Framework issued by CITRA", it also includes any data that can be used to gain access to the identity of any person. It is divided into seven sections as follows: Personal Identification, Contact Data, Marketing and Communications Data, Behavioral Data, Technical Data, Group Data, Special Categories of Personal Data.

1. **Personal identification data:** First name, last name, job title, job duties, employer, marital status, gender (inferred from the title), contact type or username.
2. **Contact data:** work phone number, mobile phone number, home phone number, work fax number, work email address, personal email address, alternate email address, work address, or area postal code.
3. **Marketing and communications data:** the user's preferences for online shopping from the service provider or their affiliated centers, and the user's communication preferences, including the preferred language for such communications.
4. **Behavioral data:** Information elicited or assumed by the service provider related to the behavior and interests of users and based on their online activities. This includes all information related to filling out forms on the service provider's website, or the user downloading materials (for example, but not limited to, technical documents, e-books, case studies and other documents or studies or papers) from the provider's website. This also includes the user's activity related to e-mail messages sent by the service provider to the user (such as "openings procedures", "clicks" and "canceling subscriptions"), and the activity of his visit to the provider's website (the pages the user has visited, including the pages on the websites of third parties), and the user's activity related to events (for example, but not limited to, attending seminars or trade fairs and anything else that resembles that on the internet which the provider sponsors, hosts, or has been involved in, and in which way).

5. **Technical data:** Internet Protocol (IP) address, user login data (including user ID and password), browser type and version, time zone setting, location, browser plug-in types and versions, operating system, platform, and other technology on the devices used to access the services of the service provider.
6. **Aggregated data:** It is the data that the service provider uses to participate in statistical data. It is extracted from the personal data collected on the condition that the identity of the user is not directly or indirectly inferred.
7. **Special categories of personal data:** Private data related to race, origin, religion, sect, philosophical beliefs, political opinions, membership (trade unions or associations of public interest) or data related to health and genetic and vital data.

Subscriber content: means any data provided or produced by a cloud computing subscriber that is saved or processed on the cloud in accordance with the cloud computing contract.

Service credits: It refers to the compensation mechanisms provided by a cloud computing service provider to its subscribers if the service provider's performance does not meet the standards stipulated in the cloud computing contract or service level agreement (SLA), or that are required under the provisions of this framework.

Data classification: The classification (or placement or arrangement) of the data according to the appropriate levels of security based on its sensitivity to determine the best means for its circulation and protection from risks.

Data owner: May be an individual, government agency or one of its sectors, or a private company or one of its sectors, where the owner owns certain data and has the authority to process, amend, copy or store it (for example, but not limited to, the human resources sector owns the entity's employees data, the information systems sector owns the infrastructure data and some systems, the financial affairs department owns the salary data, the customer service department owns the auditors' data, the supplies department owns the purchase data, etc.).

Public Cloud: The cloud infrastructure provided for public use by subscribers. This structure may be owned, managed, and operated by a commercial, academic, or governmental entity, or a combination of them. To be available on the site and/or in the center of the service provider.

Private Cloud: The infrastructure of the cloud is provided for the exclusive use of one entity or company that includes many users (for example: departments and departments managed by that entity or company) and operated by the same entity / company, or by a third party (such as: a provider of cloud computing services), or both, and its physical location may be inside or outside the headquarters of the entity / company. The data copying process is managed by the entity / company itself, and in this case developing solutions consumes more time because all deployment and testing processes need to be implemented within the entity / company.

Community Cloud: The cloud infrastructure is provided for exclusive use by a specific group of subscribers belonging to entities / companies that have common / compatible interests (for example: entity / company functions, cybersecurity requirements, and compliance considerations). This infrastructure may be owned, managed, and operated by one or more entities / companies included in that group, or a third party (service provider), or both, and its

physical location may be inside or outside the entity / company's headquarters. The service provider manages the data copying process (in fulfillment of the service level agreement (SLA) between the service provider and the entity / company) as this model supports the acceleration of the mechanism of installation and immediate operation, which leads to the acceleration of the deployment of new solutions.

Hybrid Cloud: The infrastructure of this type of cloud is a combination of two or more infrastructures of the types of cloud computing mentioned (private, public, or community) where each structure remains unique in itself and its characteristics but linked to each other. Some with standardized technology or proprietary technology that enables the connection between each cloud infrastructure in addition to enabling data and application transfer. For example: A private cloud platform might be transformed into a public load balancing platform between linked cloud computing platforms.

Migrating to the cloud: The process of transferring data or workloads, databases, applications, and information systems work procedures to the cloud, or from one cloud to another.

Cloud operating environment: The environment that manages one or a group of virtual computers through a virtual environment. The quality of the cloud operating environment depends on the cloud computing services used as well as the virtual environment type used.

Virtual machines: A simulation system for a specific computer system, this system operates based on the available computer architecture and the supposed working method of this simulated computer system. Virtual computers create a virtual environment located between the user and the platform.

Data center: A department within an organization that hosts and maintains its back-end IT systems, data storage, its large computers, their servers, and databases. In times of large central IT operations, this department and all systems are in one place and are called the data center.

Encryption: The process of converting data from readable text to unreadable text, and the encryption process is applied either during data storage or when it is transferred over networks.

Data breach: the ability to access, intercept, disclose, leak, or steal data from systems or databases without the knowledge or consent of the data owner through security holes.

Cloud Computing Regulatory Framework

Chapter 1: Scope

1.1 All provisions contained in each chapter of this framework are considered binding regulations in the area concerned, unless otherwise indicated.

1.2 The regulations of the Cloud Computing Regulatory Framework apply to all cloud computing service providers licensed by CITRA and who have data centers within the State of Kuwait and host third and fourth level data.

1.3 The regulations of the Cloud Computing Regulatory Framework apply to all cloud computing service providers registered and approved by CITRA and who host first and second level data for all public sector subscribers.

1.4 Regulations under the Cloud Computing Regulatory Framework apply to all public sector subscribers of cloud computing services, and private sector subscribers who host governmental data.

1.5 Any obligations arising from Article 1.2 as a result of contracts entered between cloud computing service providers and subscribers will be binding and obligatory on service providers.

1.6 The permanent or non-permanent storage of subscribers' data and contents with cloud computing service providers who host third and fourth level data who have data centers within the State of Kuwait and who are authorized by CITRA shall be subject to the following provisions regardless of the place of residence or location of the subscribers:

1.6.1 Article 4.2.2 of Chapter 4 (Cybersecurity for Cloud Computing), about reporting information security violations.

1.6.2 Article 4.3.3.1 of Chapter 4 (Cybersecurity for Cloud Computing) on the disclosure of subscriber's content or data to security or intelligence agencies in accordance with the laws of the State of Kuwait.

1.6.3 Article 5.1.2 of Chapter 5 (Information and Data in Violation to Laws and intellectual Property Rights), which is concerned with removing content that violates laws upon the request of CITRA.

1.6.4 Article 5.1.3 of Chapter 5 (Information and Data in Violation to Laws and Intellectual Property Rights), which is concerned with the service providers informing CITRA of any content that violates the laws.

Chapter 2: Licensing of Cloud Computing Service Providers

2.1 Those who are licensed by CITRA and who directly or indirectly have a data center and infrastructure within the State of Kuwait may enter any contracts to provide cloud computing services to the public sector within the State of Kuwait.

2.2 The licensing procedures, obligations of cloud computing service providers, and the documents required to register and obtain permission, or a license are detailed in the document "Cloud Service Providers Regulations and Commitments" on CITRAs website.

2.3 Cloud computing service providers who have obtained the necessary license from CITRA must abide by this framework in their contracts with subscribers.

2.4 CITRA grants a license to cloud computing service providers who host the third and fourth data levels, and who have data centers within the State of Kuwait.

2.5 Cloud computing service providers may register on CITRAs website to obtain permission to provide their services to subscribers from the public sector who host the first and second data levels.

Chapter 3: Data Classification

3.1 General Provisions

3.1.1 Persons who are willing to purchase cloud computing services must review and comply with the data classification policy issued by CITRA, as the data classification process is the first pillar of the process of migrating to cloud computing, as it contributes to knowing the data that can be transferred to the cloud and knowing its sensitivity and ways to protect it and choosing the appropriate cloud computing model.

3.1.2 The ownership, access and modification of subscriber's data and content is an absolute right of the subscriber. The service provider has no right to view or modify such data, transfer, delete or seize it without permission from the data owner.

3.1.3 The implementation of what is stated in the Data Classification Policy and the provisions of this chapter shall be taken into consideration without prejudice to any laws of the State of Kuwait that may be applied to shared data and content that requires a higher level of information security and protection (for example, the subscriber's data that falls within the fourth level and is required by the security entities or other concerned entities in the country).

3.1.4 This framework is without prejudice to any laws, regulations, directives, codes of conduct, internal instructions, implementation policies, or other organizational or administrative rules in force in the State of Kuwait relating to the following:

3.1.4.1 Cloud subscribers have the right to seek assistance from cloud computing service providers located outside the jurisdiction of the country, or to transmit, process, or store shared content, or any data or information in the cloud system, if data and content does not fall under the third or fourth level of data classification levels.

3.1.4.2 Second level data can be hosted using the public cloud if it meets the encryption requirements and standards, and follows the minimum-security requirements when hosting, having that the encryption keys are only available with the public cloud user.

3.1.4.3 The third level data must be stored and processed in private or hybrid cloud (public/private) models.

3.2 Data Classification Responsibility

3.2.1 As stipulated in the data classification policy, the responsibility for classifying data and content of subscribers and applying the appropriate level of data protection and security is on the subscribers of cloud computing services as follows:

3.2.1.1 Subscribers who are individuals residing in the State of Kuwait: Knowing how service providers can provide a secure cloud computing environment that meets the security requirements of their data and content according to the classification levels they choose.

3.2.1.2 Subscribers from the private and business sector:

3.2.1.2.1 Classify their data, subscribers' personal data, and government entities data that they own, and determine their security levels and methods of protection.

3.2.1.2.2 Obligation not to store or host personal data of individuals or government entities data which they have that fall within the third and fourth level of data classification on the data center and cloud computing environment of the cloud computing service provider who are outside the State of Kuwait. Hybrid clouds may be used if the data classified according to the third level within the borders of the State of Kuwait.

3.2.1.3 Subscribers from the public sector:

3.2.1.3.1 Classifying their data and the personal data of individuals and private sector companies that they have and determining their security levels and methods of protection.

3.2.1.3.2 Obligation not to store or host personal data of individuals, government entities data, or private sector companies' data that fall within the third and fourth levels of data classification on the cloud computing service provider's data center and cloud environment outside the borders of the State of Kuwait. Hybrid cloud can be used if the data that is classified according to the third level is within the borders of the State of Kuwait.

3.2.2 The subscribers of cloud computing services must choose the level of information security that commensurate with the levels of classification mentioned in The Data Classification Policy or according to what the subscriber prefer the appropriate type of data or the content of the subscriber, or if the subscriber deems it feasible to use the information protection framework that may be provided by the service provider, and which is commensurate with the subscriber's specific needs, obligations, duties and security requirements.

3.2.3 Cloud computing services subscribers must fully implement all security requirements related to classifying each level of their data or subscriber content either partially or completely.

3.2.4 Subscribers of cloud computing services, after completing the data classification process, must ensure that the following is completed:

3.2.4.1 Confidentiality: restricting access to data only to authorized people for specific purposes.

3.2.4.2 Information Integration: Ensuring that the information created, modified, saved, or circulated, only by permissible means, remains correct and usable.

3.2.4.3 Availability of information: The availability of information to authorized users and to have access to it for authorized purposes when needed.

3.2.5 The responsibility for providing and protecting a secure cloud computing environment to host the data and content of subscribers according to their categories and according to the levels of classification, security and protection of data and content that the subscribers select, lies on the provider of cloud computing services in accordance with the obligations mentioned in chapter 4 below (Cybersecurity for Cloud Computing) and in the Cloud Service Providers Regulations and Commitments document referred to in Chapter 2 (Licensing of Cloud Computing Service Providers) of this framework.

Chapter 4: Cybersecurity for Cloud Computing

4.1 General Provisions

4.1.1 This chapter introduces the minimum obligations of subscribers and cloud computing service providers towards the cybersecurity of cloud computing with respects to information security and the protection of subscribers' data.

4.1.2 This chapter aims to guide subscribers of cloud computing services in the State of Kuwait to know the importance of the location of their data and content as subscribers and what are the obligations of the service provider in the event of any violations of their data and the security responsibilities on them, depending on the type of service.

4.1.3 The cloud service provider must inform any subscriber, upon his request, of the information security features provided by the cloud service provider or that apply to the subscriber content. Cloud service provider can also fulfill this obligation by making such information available on the Internet to the subscribers.

4.1.4 Cloud services providers and their subscribers, whether they are from the government entities category or from the private sector category, are obligated to refrain from using personal data to infer the identity of subscribers without obtaining clear and explicit written permission from the individuals who own the following data: personal identification data, contact data, marketing and communications data, behavioral data, technical data, aggregated data, special categories of personal data.

4.2 Information Security

4.2.1 Subscribers' Data and Content Residency and Transfer

4.2.1.1 Subscribers of cloud computing services must ensure that no data or content is hosted or stored, in which the data classification policy and chapter three on data classification of this framework does not allow it to be hosted or stored outside the State of Kuwait for any purpose, or in any form, whether temporarily or permanently as follows:

4.2.1.1.1 Data that are classified under the third and fourth levels of data classification.

4.2.1.1.2 Data or content of government entities that fall within the fourth level of classification level.

4.2.1.1.3 Personal data of individuals held with government agencies, private sector companies, or service providers, as stipulated in article 4.1.4.

4.2.1.2 Subscribers of cloud computing services must not transfer, store, or process shared content to any public, hybrid or community cloud, unless the cloud computing service provider is properly registered and licensed by CITRA in accordance with the provisions of Chapter 2 of this framework and the Cloud Service Providers Regulations and Commitments document.

4.2.1.3 Providers of cloud computing services who are licensed by CITRA under the provisions of Chapter 2 of this Framework, concerned with the licensing of cloud computing service providers, must disclose the following to CITRA:

4.2.1.3.1 Locations and technical information of its data centers within the State of Kuwait.

4.2.1.3.2 The countries in which the providers' data centers are located if those centers are in use to process or transmit data or content of subscribers who are in the State of Kuwait.

4.2.1.4 Without prejudice to the provisions of this chapter imposed on them, cloud computing service providers are obligated to inform their subscribers in advance and obtain their prior consent, before transferring or processing their content permanently or temporarily outside the State of Kuwait.

4.2.1.5 The cloud computing service provider must comply all technical, administrative, and procedural requirements, regulatory regulations and policies issued or to be issued by CITRA in relation to its data center, directly or indirectly which are located in the State of Kuwait.

4.2.2 Reporting Information Security Violations

4.2.2.1 The cloud computing service provider must notify its subscribers within a period not exceeding seventy-two (72) hours, without undue delay, of any information security breach or data leakage as soon as the service provider becomes aware of such breach; whether such violation affects or is likely to affect subscriber content, data, or any cloud computing services provided to those subscribers by the service provider.

4.2.2.2 The cloud service provider must notify the CITRA within a period not exceeding seventy-two (72) hours, without compelling delay, of any information security breaches or data leaks of which they are aware; if such breaches or leaks affect or are likely to affect:

4.2.2.2.1 Subscriber content or data related to many cloud computing subscribers in the State of Kuwait.

4.2.2.2.2 A large group of people in the State of Kuwait, due to their dependence on the services of one or more cloud computing subscribers affected by the data leak or information security breach.

4.2.2.3 Cloud service providers must adopt internal rules and policies on business continuity, disaster recovery, and risk management. As well as providing subscribers of cloud computing service and other service providers who cooperate with them - upon their request - with a summary of these rules and policies.

4.3 Protection of Subscribers' Data

4.3.1 The provisions of Article 4.3, in addition to the Data Privacy Protection Regulation issued by CITRA, must be binding on cloud computing service providers who make a cloud computing contract with cloud computing service subscribers.

4.3.2 The cloud computing service providers are required to protect the subscribers' data and contents that falls under the third and fourth levels of data classification of the data that are hosted in the cloud computing environment, that are managed and ensure that it is encrypted so that it does not indicate the identity of the owner of this data and may not be given to other parties without permission from the owner of this data.

4.3.3 In the event of compliance with the judicial laws of a foreign country with respect to subscribers of cloud computing being subjected to the laws of that country, then the provider of cloud computing services must not:

4.3.3.1 Provide or authorize - including without limitation - any persons, legal entities, domestic or foreign government, or public authorities; any content or data related to the subscriber of cloud computing to another party.

4.3.3.2 Process or use content or data belongs to a cloud computing subscriber for purposes other than those permitted under the cloud service provision agreement with the relevant subscriber.

4.3.4 The service provider may disclose the subscriber's content or data only in the following cases:

4.3.4.1 Based on an official request from the security or intelligence authorities, in compliance with the laws enforced in the State of Kuwait.

4.3.4.2 Upon the subscriber's approval for the service provider and when the data is not within the third and fourth levels of data classification, also the subscriber has the right to cancel this approval in the future.

4.3.5 Service providers shall grant subscribers the right and technical ability to access, verify, correct, and delete their data; without prejudice to the rights of the cloud computing service providers in relation to subscriber data if this is necessary: for subscriber billing purposes, or for the purpose of fulfilling the obligations of cloud computing service providers in accordance with any of the applicable laws.

4.3.6 The provisions of Article 4.3.4 above shall apply without prejudice to any applicable statutory, regulatory, or contractual provisions; in a way that provides a high degree of protection and related rights and obligations with regard to any categories of personal, commercial, or part of subscriber data that are covered by these regulatory controls.

Chapter 5: Information and Data in Violation to Laws and intellectual Property Rights

5.1 The provisions of this chapter apply to cloud service providers, who provide the Platform-as-a-Service (PaaS) model or the Software-as-a-Service (SaaS) model, or both as cloud computing services, and who have entered into a cloud computing contract with their subscribers, in addition to those who, although they are not a party to a cloud computing contract with the relevant subscriber, either individually or jointly with others, but they exercise control over the processing of the relevant "subscriber's content" with the following:

5.1.1 The above mentioned cloud service provider shall bear any administrative or criminal liability under this framework or any regulation, decision or instructions, including the relevant laws; if the cloud service provider knows that the subscriber's publicly available content violates laws, or violates the intellectual property rights of the authors and related rights (Law No. 22 of 2016 Concerning Copyright and Neighboring Rights); when it has been uploaded, processed, or stored in the cloud of the cloud service provider, and the cloud service provider has not notified CITRA or the competent entities in the state.

5.1.2 If CITRA orders the cloud service providers in writing to remove any content that violates the laws or infringes any intellectual property rights of others from any data center or any other element of the cloud computing system located in or outside the State of Kuwait that is used or dependent on the service providers to provide cloud computing services, the service providers must ensure that content that violates or breaches any intellectual property rights of others:

5.1.2.1 Has been removed from any data center or any other component of the cloud computing environment located in or outside the State of Kuwait.

5.1.2.2 Or making it inaccessible in the State of Kuwait (if this is required under Kuwait's international obligations (and / or any other competent authority).

5.1.2.3 Cloud service providers, on their initiative, or at the request of a third party, may remove or render access inaccessible in the State of Kuwait, and / or in any other country; for any shared content that violates or infringes the intellectual property rights of third parties from their cloud computing system, provided that:

5.1.2.3.1 This must be in accordance with the provisions of the cloud computing contract.

5.1.2.3.2 The cloud service provider provides adequate notice to the affected cloud service subscribers.

5.1.3 The cloud service providers are required to inform CITRA without undue delay if they discover the presence of any content or any other information in the cloud that may violate the applicable laws.

5.1.4 The cloud service providers must refer any third party who has a complaint against contradictory content or content that infringes the intellectual property rights of others in their cloud to the competent authorities in the State of Kuwait unless they decide to address this complaint directly in accordance with paragraph 5.1.2.3 above.

5.1.5 The cloud computing service providers have the right to notify the subscriber that their own content has been found in violation of laws, or that the content violates the intellectual property rights of others in its cloud computing system and that it has been removed. Unless CITRA or any other competent authority prevents the provider of cloud computing services from doing so. CITRA and / or any other competent entity may not prevent the cloud service provider from doing so without providing a justification for that, especially if the cloud service provider fails to notify the subscriber of the content being removed, it threatens to create a liability for the cloud service provider.

5.1.6 The provisions of this chapter will be applied without prejudice to the obligation of the cloud service provider; in cooperation with the responsible entities in the State of Kuwait in accordance with any applicable regulations or instructions, or any commitment embedded in the registration procedures with CITRA in matters of

implementing regulations related to content that violates laws or content that infringes the intellectual property rights of others.

5.1.7 The cloud computing service provider must grant their subscribers all necessary legal licenses to use any software, or any other intellectual property work provided under the cloud computing contract in proportion to the term and scope of that contract.

Chapter 6: Cloud Computing Contracting

6.1 Before signing the contract with the subscriber, the service providers must provide clear and transparent information regarding the service subject, terms of use, service levels, and the payment mechanism that will be applied to the subscriber.

6.2 The obligation referred above must be applied without prejudice to any other additional information that the cloud service provider may need to communicate with subscribers; if this is required under the applicable rules or the obligations mentioned in the Cloud Service Providers Regulations and Commitments document attached to this framework.

6.3 Cloud computing requires a shared responsibility for the security and reliability of the service between service providers and subscribers. To work in this field, the subscriber must carefully consider the record and achievements of the service provider over the years, as well as the subscriber experience in the public and private sectors. The service provider should give examples of their successful projects that they have implemented to demonstrate their record in providing services in the field of cloud computing.

6.4 Without prejudice to any other obligations stipulated in the chapters of this framework, the following elements must be covered in contracts and in the service level agreements (SLAs) when contracting with cloud service providers, and service providers shall commit to absolute transparency in each of the following:

6.4.1 Identifying the cloud service provider, business address, and full details of the contact information.

6.4.2 A statement of the services to be provided and their permitted uses.

6.4.3 Terms of the cloud computing contract (if applicable), applicable fees, payment terms and termination of the contract.

6.4.4 Rules relating to the handling of subscribers' content, including its processing, to enable a cloud computing subscriber to return it to its original source upon termination of the cloud computing contract.

6.4.5 Procedures for resolving subscribers' complaints:

6.4.5.1 Cloud service provider shall offer its subscribers a customer care and support service to resolve any complaints related to them. This service should not be prejudiced by any legal treatments and other dispute

settlement procedures available under the legal systems in the State of Kuwait, in addition to this framework.

6.4.5.2 Cloud computing service providers and subscribers have the right to refer their disputes, collectively or individually, to any dispute resolution procedures available by CITRA and in accordance with its regulations, without prejudice, for example any other alternative procedures for settling disputes, or the provisions of the law that may be followed according to the applicable law.

6.4.6 The applicable system for interpreting a cloud computing contract, is to be understood that it is not allowed for the applicable system to interpretate any cloud computing contract and resolute of any dispute (if this system differs from the prevailing systems in the State of Kuwait) may invalidate any of the provisions of this framework, or any other mandatory regulations applied in the State of Kuwait that may not be revoked by choosing other international systems.

6.4.7 Data protection and privacy: the contract must contain appropriate clauses to enable subscribers from government entities or private companies contracted with them to fulfil their obligations towards personal data (for example: ensuring that all personal data is dealt with in accordance with privacy laws, data protection in force and work. With the Data Classification Policy and what is stated in this framework).

6.4.8 Security and data breach protocols: the contract must contain obligations from the service provider to ensure the security of information and data. The contract must state what happens in the event of a data breach, in addition to the notification procedures in place.

6.4.9 Ownership of data: the subscribers' data must remain their property and not be the property of the service provider.

6.4.10 Use of data: the contract must clarify that the data will be used only for purposes related to providing cloud computing services and not for secondary purposes, such as advertisements, except with the consent of the subscriber.

6.4.11 Data Access: subscribers reserve the right to direct access to data at any time upon request, and they reserve the right to control who can access their data and the conditions related to that.

6.4.12 Monitoring and Control: the contract should contain obligations from the cloud computing service provider to monitor and control the services provided and the associated reports.

6.4.13 Service Availability: subscribers must ensure the commitment of the service provider to provide the necessary guarantees of service availability, and providing specific and necessary repairs in the event of a sudden and unscheduled service failure.

6.4.14 Subcontracting: the contract should contain provisions to ensure that if the service provider contracts with any subcontractor, it works to fulfil the main contractual obligations, and the final responsibility for performance must fall on the service provider.

6.4.15 Business continuity: to ensure that business continuity is met, the contract must provide a disaster recovery plan and with appropriate continuing testing processes.

6.4.16 Confidentiality: subscribers must ensure that the cloud service provider makes obligations regarding the confidentiality of information stored within the cloud.

6.4.17 Contract cancellation and exit: subscribers must obtain guarantees confirming their right to cancel cloud computing services after agreement with the service provider, with the ability to transfer data to another service provider or to another data center, with the service provider's commitment to the following:

6.4.17.1 The subscriber's cloud computing content is provided to the subscriber's service provider with a copy of the subscriber's cloud computing content saved in the service provider's cloud computing system at the time of terminating the cloud computing service contract in the form used by convention.

6.4.17.2 Providing the cloud computing subscribers with the means that enable them to recover their content in the form used by convention.

6.4.17.3 Deleting the subscriber's content from the cloud of the service provider upon the subscriber's request after he receives copies of the cloud content upon the termination of the contract and the exit.

6.4.17.4 As an alternative to the above options the service provider may transfer the subscriber's cloud content using an appropriate format directly to another service provider chosen by the cloud computing subscriber, whenever this is technically possible.

6.4.17.5 The service provider, upon the request of the government entity, is obligated to hand over the content of the data owned by the government entity and hosted by the service provider in any classification, and is not entitled to refrain from delivering such data or keep a copy of this data on the grounds that the dispute is still ongoing or that there are financial payments that have not been made upon requesting data, and the service provider may not obstruct the transfer of government services on the pretext that the dispute is still ongoing or that there are unresolved financial payments.

6.4.17.6 The service provider is obligated to ensure the continuity of services in the government entity during a dispute for a period of no less than 6 months from the start of a conflict situation until securing the government entity from moving to another service provider, and the service provider may not

obstruct the transfer of government services on the pretext that the dispute still exists or there are unreconciled financial payments.

Chapter 7: Protecting Subscribers from Unfair Contract Terms

7.1 The cloud service provider shall be held accountable to its subscribers, for any acts or negligence, agents, subcontractors, or employees (who act within the framework of their agency, function, or subcontract with the service provider) in accordance with the provisions of this article or any other regulations in force in the State of Kuwait, regardless of whether those acts or negligence occurred inside or outside the State of Kuwait.

7.2 Cloud service providers must not be entitled to exclude their liability stipulated in the contract - in front of their subscribers – regarding subordinate individuals as a result of the losses and damages mentioned below. If those losses and damages can be logically attributable, in whole or in part, to intentional acts, negligence or omission from before the service provider.

7.2.1 Any loss or damage to the subscriber's content or data, if this is related to the processing of the cloud service provider, or any other interaction with that subscriber's content or data.

7.2.2 Quality, performance, accessibility, service downtime, or other similar service standards that do not match the service provider's obligations under the cloud computing contract with the concerned subscriber, or with any other mandatory statutory provisions.

7.2.3 Any information security breach.

7.3 The "best endeavors" clause will not be effective if service providers use it in their cloud computing contract, service providers shall be held accountable to cloud computing service subscribers due to acts or omissions committed intentionally or due to gross negligence.

7.4 Cloud computing subscribers are responsible for proving that any loss or damage referred to in paragraphs 7.1, 7.2 and 7.3 is logically attributable, in whole or in part, to intentional acts, negligence, or omissions on the part of the cloud computing service provider.

7.5 Notwithstanding the above, cloud computing service providers may:

7.5.1 Exclude or limit their liability for any indirect damages, loss of revenue, or profit if this happened unintentionally to the subscriber of the cloud.

7.5.2 Limit their liability to reasonable peak that may include, other alternatives, and the sum of fees paid or owed to the cloud service subscriber under contract with the cloud service subscriber and / or compensation to the cloud service subscriber through service credits.

7.6 Without restricting Article 7.5, cloud service providers can exclude or limit their responsibilities to non-individual cloud subscribers to the extent they agree with those subscribers under the cloud computing contract.

Chapter 8: Quality Control Standards

8.1 Registered service providers who have permission or who are licensed by CITRA must:

8.1.1 Notify their subscribers, upon request, of any system or certification standards that service providers meet in relation to the relevant cloud computing services.

8.1.2 Obtain a written consent from their subscribers before transferring or copying their data outside the State of Kuwait, explaining the reasons, and specifying the party to which the data is to be copied or transferred as long as it does not fall within the third and fourth level of data classification.

8.1.3 They shall comply with any approval plans and / or standards (including coding standards) which may be defined as mandatory by a decision from CITRA regarding the type of cloud computing service provided by the service provider.

8.1.4 They shall abide by any rules or guidelines approved by CITRA regarding business continuity, disaster recovery, and risk management.

8.2 The encryption process by the cloud subscriber of their data or content; shall not affect the obligations of cloud service providers under this framework.

8.3 CITRA may from time-to-time issue decisions regarding mandatory or optional accreditation plans and standards for cloud computing, which may differ according to the required level of information security, the type of cloud service provider, the concerned computing subscriber, or other criteria.

Chapter 9: The Communication and Information Technology Regulatory Authority Powers

9.1 Any breach of the provisions of this framework, or other policies and regulations issued by CITRA be subject to penalties that may be imposed by CITRA under the law of its establishment without prejudice to any penalties and any other laws applied in the State of Kuwait, as well as other provisions that may be amended or replaced in the future.

9.2 CITRA has the right to issue guidelines, model cloud computing contracts, materials, policies, regulations, recommendations, or other documents aimed for:

9.2.1 Regulating the use of cloud computing in the State of Kuwait.

9.2.2 Provide guidance and obligations to cloud service providers, cloud subscribers, governmental entities, and the private sector, in general, on any aspects of cloud computing.

9.2.3 Amendment to the chapters and articles of this framework without prior notice.

Chapter 10: Implementation of Transitional Measures

10.1 This regulatory framework for cloud computing comes into effect 30 days after the date of its publication in the official newspaper.

10.2 A grace period of six months, from the date in which the Cloud Computing Regulatory Framework is into effect and is given to subscribers and cloud computing service providers to amend their status in accordance with the provisions of this framework and to the Cloud Service Providers Regulations and Commitments document attached to this framework.

10.3 The obligation of cloud service providers to register and obtain the necessary permission or licensing from CITRA will come into effect within (30) days from the date of this framework coming into effect.

Chapter 11: Final Provisions

11.1 CITRA may amend the provisions of this framework, if required, and the proposed amendment shall be submitted to the board of directors for approval.

11.2 In the event of a proven violation of the provisions of this framework, CITRA may apply the penalties and fines stipulated in its establishment Law No. 37 of 2014, as amended by Law No. (98) of 2015.

Chapter 12: Appendix

The document mentioned below is considered an appendix to this framework and can be found on the official website for the Communication and Information Technology Regulatory Authority (CITRA): (www.citra.gov.kw)

12.1 Cloud Service Providers Regulations and Commitments

Chapter 13: Related Documents

The documents listed below are linked to this framework and can be reviewed through the official website of the Communication and Information Technology Regulatory Authority (CITRA): (www.citra.gov.kw)

13.1 Data Classification Policy

13.2 Cloud First Policy

13.3 Data Privacy Protection Regulation

13.4 ICT Terms and Definitions