هيئة الاتصالات والفضاء والتقنية
Communications, Space & Technology Commission

Cloud Computing

Regulatory Framework

Version (3)

RS10

Table of Contents

1 Introduction

1-1 According to Article Three of the Communications Law (hereinafter referred to as the "Law"), the communications and information technology sector shall be regulated - among other objectives - by creating and encouraging an appropriate climate for fair and effective competition in all areas of communication and information technology.

1-2 Cabinet Resolution No. (133), dated 21/05/1424H added the powers of the Communications and Technology Information Commission (hereinafter referred to as "CITC") to include the field of information technology, and entrusted it with tasks which include, but not limited to, the following:

1-2-1 Implementing the approved policies, plans, and programs for developing information technology, and setting appropriate procedures;

1-2-2 Proposing regulations related to information technology and amendments thereof, and working on their approval by the competent authorities; and

1-2-3 Issuing the necessary licenses in accordance with the relevant terms and regulations.

1-3 Cabinet Resolution No. (292), dated 27/04/1441H, in Article Seven, affirmed the continuation of the Ministry of Communications and Information Technology and CITC in accordance with its powers stipulated in the Communications Law and CITC's Statute in regulating the matters related to information technology, including cloud computing.

1-4 The communications and information technology sector is currently witnessing rapid change, and CITC's adoption of this "Cloud Computing Regulatory Framework" will result some benefits through enhancing cloud computing services in the Kingdom of Saudi Arabia (hereinafter referred to as the "Kingdom"), and providing adequate regulatory transparency.

2 Definitions:

2-1 Terms and expressions defined in the Law and its Implementing Regulations shall have the same meanings when used in this Regulatory Framework.

2-2 The following terms and expressions shall have the meanings set forth in front of them as follows:

2-2-1 "Cloud Computing" means the use of a pool of flexible, scalable and sharable physical and virtual resources (for example, servers, operating systems, networks, programs, applications, and storage equipment) in addition to providing and managing services automatically upon request.

2-2-2 "Cloud Computing Services" or "Computing Services" means providing information and communication technology services through cloud computing, which includes, but is not limited to, storing, transmitting, or processing subscriber content in a cloud computing system. Cloud computing services are divided into three basic services:

2-2-2-1 Software as a Service (SaaS) The services provided to cloud computing subscribers to use the cloud service provider applications that run on cloud platforms and infrastructure. Applications can be accessed from different cloud computing subscribers' devices through a server-based software interface (thin client), similar to a web browser (such as the web-based email). A subscriber does not manage or control the underlying cloud infrastructure that includes the network, servers, operating systems, storage, or even individual application capabilities, except perhaps for some user-specific application configuration settings. Examples may include, but are not limited to, Enterprise Resource Planning (ERP) systems, Customer Relationship Management (CRM) systems, and communications software (e-mail and instant messaging).

2-2-2-2 Platform as a Service (PaaS) The services provided to cloud computing subscribers in publishing applications developed or

purchased by the consumer from a cloud service provider on cloud platforms and infrastructure. These applications are developed using programming languages and tools that are supported by the cloud service provider, and the consumer does not manage or control the platform and the underlying cloud infrastructure which includes the network, servers, operating systems, or storage. However, the consumer controls published applications and possibly application hosting environment configurations. Examples may include, but are not limited to, application development, databases and a database management system (DBMS), testing tools and developer tools.

2-2-2-3 Infrastructure as a Service (IaaS) The primary computing resources (processing, storage, networking, etc.) provided to subscribers of cloud computing. The subscriber is free to choose the software to be published and run, which may include operating systems and applications. The subscriber does not manage or control the underlying cloud infrastructure, but rather the operating systems, storage and published applications, and may have limited control over some network components (such as security systems). Examples may include, but are not limited to, virtual machines, mainframe computers, IT facilities / hosting services.

2-2-3 “Cloud Computing Service Provider” means any person who provides cloud computing services to any entity or individual, whether directly or indirectly, such as a service provider, service broker, service aggregator, service reseller provider, or service provider agent; and this is as follows:

2-2-3-1 "Service Provider” means any person who provides cloud computing services to any entity or individual through data centers owned and managed partially or completely by the same person.

2-2-3-2 "Cloud Computing Service Broker” means any person acting as an intermediary between one or more cloud computing service providers and cloud computing subscribers.

2-2-3-3 "Cloud Computing Service Aggregator” means any type of cloud computing brokers who aggregate and combine many of their services into one or more combined packages they provide to cloud computing subscribers.

2-2-4 "Cloud Computing Subscriber" means any person to whom the cloud computing service provider agrees to provide his services under a "cloud computing contract" or other commercial relationship between the service provider and such person.

2-2-5 "Cloud Computing User" means any natural person (individual) who uses the services of the cloud computing service providers provided to the cloud computing subscriber according to the relationship between such subscriber and the cloud computing user. This individual may be a user and a subscriber at the same time, if a "cloud computing contract" is concluded to provide "computing services" to a single cloud individual "user".

2-2-6 "Cloud Computing Nodes" means any agreement entered into between a cloud computing service provider and its subscribers to provide such services.

2-2-7 "Cloud Computing System" means the electronic information system which includes hardware, software and network elements owned, controlled, operated, leased or otherwise from the resources the CSP relies on to provide its services to cloud computing subscribers. A cloud computing system may include one or more data centers, among other things.

2-2-8 "Public Cloud Computing" means any cloud computing system available for open use by an entity or an individual.

2-2-9 "Community Cloud" means a cloud computing system provided for the exclusive use of a closed group of "cloud computing subscribers" who share some social, business, administrative or other goals.

2-2-10 "Private Cloud Computing" means a cloud computing system available for the exclusive use of only one cloud computing subscriber.

2-2-11 "Hybrid Cloud Computing System" means any combination of two or more public, private and/or community cloud computing systems, which are linked together, whether by a standard or special technology that enables transmission of data and applications.

2-2-12 "Data Center" means the facility that contains essential cloud computing infrastructure and its supporting components, which are hosted on the same site, and are used at least partially for storing and/or processing subscriber content and data.

2-2-13 "Content" means any programs, texts, files, sound recordings, images, animations, captions, information, personal or commercial data, or any other data in any form.

2-2-14 "Subscriber Content" means any content provided or produced by a cloud computing subscriber that is saved or processed in the cloud computing system in accordance with the cloud computing contract for the purpose of providing cloud computing services through such system to the subscriber.

2-2-15 "Subscriber Data" means any data falling under at least one of the following categories mentioned below, to the extent that it is or was part of the subscriber content or previously produced by the cloud computing service provider in relation to its one or more cloud computing subscribers.

2-2-15-1 Any data related to a natural person who is specifically identified directly or indirectly as a cloud computing user, specifically by referring to an identification number or one or more elements that user is allowed to be identified by.

2-2-15-2 Any data related to business activities, business information or financial affairs of the cloud computing subscriber, including but not limited to, the subscriber's rates, employee data, products, customers, financial statements, audit data, security, commercial data, or product development data, even if such data or information is publicly available.

2-2-15-3 Any data produced by the cloud computing service provider that relates to the service subscriber activity log, billing system, usage volume, statistics, or information of his use of services provided by the cloud computing service provider.

2-2-16 "Subscriber Address" means the cloud computing subscriber address: (1) Submitted in the cloud computing service contract, or (2) the billing address, and if the two are different and only one of them is in the Kingdom, the Subscriber Address is the address which is located in the Kingdom.

2-2-17 "Third-Party Content" means any content, whether in electronic form, taken, or derived from anyone other than a cloud computing service provider or cloud computing subscriber, and provided to the subscriber through or in conjunction with a cloud computing subscriber's use of its services.

2-2-18 "Law-Violating Content" means a subscriber or third-party content that violates the Kingdom's laws.

2-2-19 "IPR-Violating Content" means a subscriber or third-party content that infringes intellectual property rights.

2-2-20 "Residence" means permanent or temporary residence in accordance with the Kingdom's laws. This does not include accommodation of people who are on a short visit to the Kingdom or on transit.

2-2-21 "Service Credits" means the compensation mechanisms provided by the cloud computing service provider to its subscribers in the event that the service provider's performance does not meet the standards stipulated in the "cloud computing service contract", or required under the provisions of this Regulatory Framework. "Service Credits" can include, but is not limited to, discounts on current or future bills, and adding time for "cloud computing services" at the end of the billing cycle for free.

2-2-22 "Service Level Agreement" means a service level agreement between a cloud computing service provider and a cloud computing subscriber that defines the quality of cloud computing services provided to the subscriber in terms of a set of measurable standards related to cloud computing.

3 The Regulatory Framework

3-1 Scope

3-1-1 The provisions of this Regulatory Framework apply in relation to the cloud computing services provided to subscribers residing in or having a subscriber's address in the Kingdom.

3-1-2 Regardless of the subscriber's residence or address, the processing or storing of the content or data of any subscriber temporarily or permanently in data centers, or in other elements of the cloud computing system, located in the Kingdom, shall be subject to the provisions listed below:

3-1-2-1 Paragraph No. 3-3-12 (Reporting major cybersecurity incidents) below.

3-1-2-2 Paragraph No. 3-5-4 and Paragraph 3-5-5 (Remove law-violating content, or IPR-violating content, at the request of CITC or any other competent authority) and Paragraph No. 3-5-6 below about (Notifying CITC of violations of Anti-Cyber Crime Law).

3-1-2-3 The exception referred to in Paragraph No. 3-4-3-1 below.

3-1-2-4 Paragraph No. 2-3 (Registration to provide cloud computing services) below.

3-1-3 Any obligations arising from Paragraph No. 3-1-1 above will be binding on the cloud computing service provider who entered into a cloud computing contract with the concerned subscriber(s).

3-1-4 Unless otherwise specified in this Regulatory Framework, these provisions shall be mandatory and not subject to any amendment during the validity of the contract agreement.

3-2 Registration to provide cloud computing services

3-2-1 No service provider has the right to exercise direct or effective control over the data center or the critical infrastructure of a cloud computing system hosted and used in the Kingdom, in whole or in part, for the purpose of providing cloud computing services, before performing the correct and complete registration with CITC; provided that it uses the communications infrastructure, including international communications, through those authorized by CITC.

3-2-2 The registration requirements and procedures described in the "Guide for Cloud Computing Service Providers in the Kingdom of Saudi Arabia" document and published on the CITC's website in its approved Arabic version shall be mandatory for those who meet the registration requirements according to what is stated in Paragraph No. 3-2-1.

3-2-3 CITC may register service providers in a qualifying category to overcome the challenges of registering them in one of the registration categories referred to in Table No. 2, provided that CITC specifies the requirements and procedures for this.

3-3 Subscriber Data

Subscriber Data Classification

3-3-1 Subscriber data may be subject to different levels of classification - depending on what is issued by the National Data Management Office or the regulatory authorities supervising the subscriber; and that depends on the required level to preserve the subscriber's data, its confidentiality, integrity and availability as indicated in Table 1 and Table 2 below, as well as subject to the provisions of Paragraph No. 3-3-4:

Table 1: Subscriber Data Classification

Subscriber Data Classification	Classification Level	Description
Data of Saudi Government Agencies	Extremely Confidential	Data is classified as (Extremely Confidential) if unauthorized access to this data or its disclosure or its content leads to serious and exceptional damage that cannot be remedied or repaired on: • National interests, including breaching agreements and treaties, harming the Kingdom's reputation, diplomatic relations and political affiliations, or the operational efficiency of security or military operations, the national economy, national infrastructure, or government business. • The performance of government agencies, which is harmful to the national interest. • Broader individual health and safety and the privacy of senior officials. • Environmental or natural resources.
	Confidential	Data is classified as (Confidential) if unauthorized access to this data or its disclosure or its content leads to serious and exceptional damage that cannot be remedied or repaired on: • National interests, including partially harming the Kingdom's reputation, diplomatic relations and political affiliations, or the operational efficiency of security or military operations, the national economy, national infrastructure, or government business. • Causes a financial loss at the organizational level that leads to bankruptcy, the inability of the entities to perform their duties, a serious loss of competitiveness, or both. • Causes serious harm or injury that affects the life of a group of individuals. • Leads to long-term damage to environmental or natural resources. • Investigating major cases as specified by law, such as terrorism financing cases.
	Restricted	Data is classified as (Restricted): If unauthorized access to or disclosure of this data or its content leads to: • A limited negative impact on the work of government agencies or economic activities in the Kingdom, or on the work of a specific person.

		• Limited damage to any entity's assets and limited loss on its financial and competitive position. • Limited damage in the short term to environmental or natural resources.
	Public	Data is classified as (Public) when unauthorized access to or disclosure of this data or its content does not result in any of the effects mentioned above - in the event that there is no effect on the following: • National interest • Entity activities • Interests of individuals • Environmental resources
Data of Non-Government Agencies	Data Received from Saudi Government Agencies: Classified as received from the government agency based on the levels specified above.	
	Other Data: Not covered by the above, provided that what is issued by the National Data Management Office or the sector regulators supervising the subscriber are taken into consideration.	

Table 2: Categories of Registration of Service Providers

(C)2	(B)	(a)	Service Provider Registration Category[1] / Data Classification	
✓			Extremely Confidential	**Data of Saudi Government Agencies**
			Confidential	
✓	✓		Restricted	
✓	✓	✓	Public	
Classified as received from the government agencies			Data Received from Saudi Government Agency	**Data of Non-Government Agencies**
✓	✓	✓	Other Data:	

Note1: The service provider registration category is the category for which the service provider is qualified to deal with subscriber data according to the subscriber data classification shown in Table 1 and Table 2. The "Guide for Cloud Computing Service Providers in the Kingdom" document explains the special requirements for each category.

[2]To deal with government agencies' data that are classified as Confidential and Extremely Confidential, it requires referring to CITC to obtain the necessary approvals in accordance with the applicable laws, regulations, policies, and governance models in the Kingdom.

3-3-2 The provisions of this Regulatory Framework shall not prejudice any laws, regulations, directives, codes of conduct, internal instructions, implementation policies, organizational or other administrative rules in force in the Kingdom related to the following:

3-3-2-1 The right of cloud computing subscribers - if any - to outsource, transmit, process, or store shared content, or any data, or

information in the cloud computing system, taking into account the requirements for outsourcing.

3-3-2-2 The obligation of cloud computing subscribers - if permitted by CITC - to ensure that the outsourcing, transmission, processing, or storage is subject to some restrictions, or preventive measures for cybersecurity - as long as they do not conflict with what is issued by the National Cybersecurity Authority - or data protection or integrity, in addition to those specified in this Regulatory Framework.

3-3-3 The service provider may exclude some or all of the cloud computing subscriber's commercial data from the definition of the subscriber's data mentioned in Paragraph No. 2-2-15, subject to the cloud subscriber's prior consent.

Subscriber Data Classification Responsibility

3-3-4 Cloud computing subscribers shall choose the appropriate data classification from among the classifications specified in Table 1 mentioned in Paragraph No. 3-3-1, or any other similar list provided for this purpose by the cloud computing service provider, which is in conformity with their security requirements, specific needs, obligations and duties. Subscribers whose data is classified as (Data of Saudi Government Agencies) shall contract with a service provider registered with CITC.

3-3-5 Cloud computing subscribers shall be responsible for implementing all cybersecurity requirements that are required to apply to any part of their content.

3-3-6 The service provider shall notify its cloud computing subscribers of the category in which it is registered with the CITC, provided that it includes the level of classification of the subscriber's data shown in Table 1 and Table 2 mentioned in Paragraph No. 3-3-1.

Subscriber Content Site and Transfer

3-3-7 The cloud computing service provider shall inform any cloud computing subscriber of the cybersecurity requirements that the cloud computing service provider provides or that apply to the cloud computing subscriber's content, and cloud computing service providers may also fulfill this

obligation by making such information available on the Internet to subscribers of cloud computing services.

3-3-8 The cloud computing service providers registered with CITC and cloud computing subscribers shall not transfer any content from the data of Saudi government agencies outside the Kingdom for any purpose, or in any form, whether permanently or temporarily (for example: temporary storage and backup, or similar purposes), unless it is expressly stated that it is permitted according to the laws or regulations in the Kingdom, except for this "Regulatory Framework".

3-3-9 Cloud computing subscribers may not transfer, store, or process shared content from Saudi government agencies' data to any public cloud computing system, community cloud computing system or hybrid cloud computing system belonging to a service provider within the Kingdom, unless the cloud computing service provider is properly registered with CITC in accordance with the provisions of Article No. (2-3) above.

3-3-10 Without prejudice to their obligations stipulated in Paragraph No. 3-3-7, cloud computing service provider registered with CITC shall clearly notify CITC and their service subscribers in advance and obtain their consent if their content will be transferred, stored or processed outside the Kingdom permanently or temporarily.

Reporting Cybersecurity Incidents

3-3-11 The cloud computing service provider shall notify its subscribers, without unjustified delay of any cybersecurity incidents, including data leakage, it is aware of, which affects or is likely to affect subscriber content, data, or any cloud computing services provided to those subscribers by the service provider.

3-3-12 The cloud computing service provider shall notify CITC and the National Cybersecurity Authority without undue delay of any cybersecurity incident or violation of cybersecurity. The cloud computing service provider shall notify CITC without undue delay of any data leakage incident (including personal data) that it is aware of - and CITC shall notify the National Data Management Office, If these violations or leaks affect or are likely to affect:

3-3-12-1 Shared content from Saudi government agencies.

3-3-12-2 A large number of people in the Kingdom due to its reliance on the services of one or more cloud computing subscribers that have been affected by a cybersecurity incident, including data leakage.

3-3-13 Cloud computing service providers shall notify cloud computing service subscribers of any insurance coverage provided by cloud computing service providers against any civil liability for these subscribers. Information relating to insurance coverage should include at least the basic characteristics as long as this may be reasonably required for cloud computing subscribers to assess their exposure to risk, and to make a decision about their insurance coverage accordingly.

3-3-14 Service providers shall adopt internal rules and policies for business continuity, disaster recovery and risk management, and shall provide cloud computing service subscribers, and its service providers who work with them, a summary of these rules and policies.

3-4 Subscriber Data Protection

3-4-1 The provisions of this Paragraph No. 3-4 are binding on cloud computing service providers who:

3-4-1-1 Enter into a cloud computing contract with the cloud computing subscriber, in addition to:

3-4-1-2 Those who specify the goals and means of processing the data of the relevant subscriber alone or jointly with others; although they are not a party to the concerned subscriber's computing contract.

3-4-2 Without prejudice to the laws of a foreign jurisdiction regarding cloud computing subscribers subject to those laws, the cloud computing service provider may not:

3-4-2-1 Provide or authorize any other party (including but not limited to any persons, legal entities, local or foreign government, or public authorities) by providing any content or data related to the cloud computing subscriber.

3-4-2-2 Process or use content or data pertaining to the cloud computing subscriber for purposes other than those permitted under the “cloud computing agreement” with the concerned subscriber. The service provider shall disclose (according to a designated detailed document) any capabilities it has to view any data stored in its

possession in the Kingdom or that has been processed or transferred in or through it, or to decode such data, or to assist any third party or allow it to view or decipher such data. The service provider shall not implement any new capabilities in this regard without obtaining CITC's explicit and prior written approval.

3-4-3 The obligations of the cloud computing service providers mentioned in Paragraph No. 2-4-2 above do not apply in relation to any subscriber's content or data that meets one of the following two conditions:

3-4-3-1 That the service providers are required by the cloud computing subscriber to disclose, transmit, process or use the subscriber's content or data in accordance with the laws of the Kingdom, or

3-4-3-2 The subscriber's data (non-governmental entities) is of another type of data, and the relevant cloud computing subscriber expresses his prior explicit consent (whether in the form of sharing or not sharing), whereby the subscriber has the right to withdraw at any time in the future.

3-4-4 Service providers shall grant subscribers the right and the technical ability to access and verify, correction and delete their data in a manner that does not contradict what is issued by the National Data Management Office regarding personal data.

3-4-5 The obligations of service providers mentioned in Paragraph No. 3-4-4 above shall be complied with, without prejudice to the rights of the cloud computing service providers in relation to the subscriber data mentioned in Paragraph 2-2-15-3 above as long as this is necessary:

3-4-5-1 for subscriber billing purposes; or

3-4-5-2 for the purpose of fulfilling the obligations of cloud computing service providers in accordance with any of the laws in force in the Kingdom.

3-4-6 The provisions of Paragraph No. 3-4 above shall apply without prejudice to any statutory, regulatory or contractual provisions applicable in the Kingdom which provide a high degree of protection and related rights and obligations, regarding any categories of personal or commercial data, or that form part of subscriber data covered by this Regulatory Framework.

3-5 Law-Violating Content and IPR-Violating Content

3-5-1 The provisions of Paragraph No. 3-5 shall apply to cloud computing service providers:

3-5-1-1 which have entered into a "cloud computing contract" with their subscribers, and

3-5-1-2 those who exercise control over the processing of the relevant "subscriber's content", even though they are not a party to the cloud computing contract with the concerned subscriber, whether alone or in association with others.

3-5-2 In accordance with the provisions of Paragraph No. 3-5, the cloud computing service provider does not assume any administrative or criminal responsibility under this Regulatory Framework or any law, regulation, decision or instructions, including the Anti-Cyber Crime Law, only based on the fact that the subscriber's content violates the law, or infringes the intellectual property rights of others, or it has been downloaded, processed, or stored in a cloud computing system of the cloud computing service provider.

3-5-3 Nothing in this Regulatory Framework shall be construed as a legal obligation on cloud computing service providers to monitor their cloud computing system, in order to identify the content violating the law, or subscriber's content that infringes any intellectual property rights of others.

3-5-4 If CITC or any other competent authority in the Kingdom has directed the cloud computing service providers in writing to remove any content that violates or infringes any intellectual property rights of others from any data center or any other element of the cloud computing system located in the Kingdom that is used or relied upon by service providers in providing cloud computing services in accordance with the provisions of Paragraph No. 3-1-1 and Paragraph No. 3-1-2 above, the service providers shall ensure that the content that violates or infringes any intellectual property rights of others:

3-5-4-1 has been removed from any data center or any other element of the cloud computing system in the Kingdom; or

3-5-4-2 make it inaccessible in the Kingdom, (if so required under the Kingdom's international obligations) and/or any other competent authority.

3-5-5 Cloud computing service providers may, on their own initiative, or at the request of a third party, remove or make inaccessible in the Kingdom and/or in any other country any subscriber's content that violates or infringes intellectual property rights of others from their cloud computing system, provided that:

3-5-5-1 this is in accordance with the provisions of the cloud computing contract; and

3-5-5-2 that the cloud computing service provider provides sufficient notice to the affected cloud computing subscriber.

3-5-6 Cloud computing service providers must notify CITC and/or any competent authority, without undue delay, if they discover the existence of any content or any other information in the cloud computing system which may be violating the laws and legislations of the Kingdom.

3-5-7 Cloud computing service providers must refer any third party - except for the competent authorities - who has a complaint regarding a violating content or a content violating intellectual property rights of others in their cloud computing system to the competent authorities in the Kingdom unless they decide to address this complaint directly in accordance with Paragraph No. 3-5-5 above.

3-5-8 Cloud computing service providers have the right to notify the subscriber that a content pertaining to him has been found as violating the law, or that his content infringes any intellectual property rights of others on its cloud computing system and such content has been removed, unless CITC or any other competent authority prevents the cloud computing service provider from doing so. CITC and/or any other competent authority may not prevent the cloud computing service provider from doing so without providing a relevant justification, especially if the failure of the cloud computing service provider to notify the subscriber of the content being removed threatens to entail any liability on the cloud computing service provider.

3-5-9 The provisions of Paragraph No. 3-5 shall apply without prejudice to the obligation of the cloud computing service provider to cooperate with the competent authorities in the Kingdom in accordance with any applicable laws or instructions, or any obligation embedded in the registration procedures with CITC in the matters pertinent to the application of

regulations related to the law-violating content or the content that infringes the intellectual property rights of others.

3-5-10 The cloud computing service provider shall grant its subscribers all necessary statutory licenses to use any software, or any other intellectual property work protected by the system and provided under the cloud computing contract in proportion to the term (if applicable) and the scope of such contract.

3-6 Information about cloud computing service contracts and the mandatory minimum content

3-6-1 Before signing the contract with the subscriber, the service provider shall provide clear and transparent information to the subscriber about the subject of the service, terms of use, levels of service, the payment mechanism to be applied, and the category in which he is registered with CITC, provided that it includes the level of classification of the subscriber's data shown in Table 1 and Table 2 mentioned in Paragraph No. 3-3-1.

3-6-2 The obligation indicated above shall be applied, without prejudice to any other additional information that may be needed by the cloud computing service provider to communicate with subscribers, if this is so required by applicable rules or obligations contained in the registration procedures.

3-6-3 Without prejudice to any other obligations stipulated in this Regulatory Framework, the cloud computing service provider shall ensure that the following information as a minimum is included in cloud computing service contracts:

3-6-3-1 Information of the cloud computing service provider, business address, and full contact details.

3-6-3-2 A statement of the services to be provided and their permitted uses.

3-6-3-3 Cloud computing contract term (if applicable), applicable fees, terms of payment and termination of the contract.

3-6-3-4 Rules related to handling subscriber content, including its processing, or the processing to enable a cloud computing subscriber to return it to its original source upon termination of the cloud computing contract.

3-6-3-5 Information regarding availability, terms and conditions of any service level agreement ("SLA") that a cloud computing service provider can make available to its subscribers.

3-6-3-6 Procedures for resolving subscribers' complaints.

3-6-3-7 The applicable law for the interpretation of the cloud computing contract, provided that it is understood that it is not permissible that the law applied for interpreting any cloud computing contract and resolving any dispute (if such law is different from the prevailing laws in the Kingdom) cannot nullify any of the provisions of this Regulatory Framework, or any other obligatory regulations applied in the Kingdom that may not be nullified by choosing other international laws.

3-6-4 Cloud computing service providers shall provide its subscribers with a customer care service to resolve any complaints belong to them. This service shall not be prejudiced by any other legal remedies and dispute settlement procedures that are available under the law, including this Regulatory Framework.

3-6-5 Cloud computing service providers and subscribers have the right to refer their disputes, collectively or individually, to any dispute resolution procedures made available by CITC and in accordance with its regulations, without prejudice to, for example, but not limited to, any other alternative procedures for resolving disputes, or provisions of the law that may be followed pursuant to the applicable law.

3-6-6 Upon terminating the cloud computing contract with a cloud computing subscriber, and if the subscriber so requests, the service provider shall:

3-6-6-1 provide the cloud computing service subscriber with a copy of his cloud computing content that is saved in the service provider's cloud computing system at the time of termination of the cloud computing service contract in the form used by convention.

3-6-6-2 Provide the cloud computing subscriber with the means that enable him to restore his content in the form used by convention.

3-6-7 As an alternative to the options mentioned in Paragraph No. 3-6-6-1 and Paragraph No. 3-6-6-2 above, the service provider may transfer the subscriber's cloud computing content to an appropriate format directly to

another service provider chosen by the cloud computing subscriber, whenever this is technically possible.

3-7 Subscriber Protection and Unfair Contract Terms

3-7-1 The could computing service provider shall bear responsibility before CITC and its individual subscribers for any acts or negligence on its part, or by its agents, or subcontractors or employees (who are acting within the framework of their agency, employment, or sub-contract with the service provider), according to what is stated in this Paragraph No. 3-7 or any other laws in force in the Kingdom, regardless of whether or not these acts or neglect may have occurred inside or outside the Kingdom.

3-7-2 The cloud computing service providers do not have the right to disclaim their liability stipulated in the contract before their subscribers for the loss and damage mentioned below, if such loss and damage could logically, wholly or partially, be attributed to intentional acts, negligence or omission by the service provider:

3-7-2-1 Any loss or damage to the subscriber's content or data, if this is related to the processing of the cloud computing service provider, or any other handling of the content or data of such subscriber.

3-7-2-2 Quality, performance, accessibility, duration of downtime, or other similar service standards that do not match the obligations of the service provider under the cloud computing contract with the concerned subscriber, or with any other mandatory statutory provisions.

3-7-2-3 Any cybersecurity incidents.

3-7-3 The "best endeavors" clause used in the cloud computing contract by will not exempt the service provider from its liability to individual cloud computing service subscribers for the acts or omission intentionally committed or are due to gross negligence.

3-7-4 Cloud computing subscribers bear the burden of proof that any loss or damage referenced in Paragraphs No. 3-7-1 and No. 3-7-2, which are logically attributable, in whole or in part, to intentional acts, negligence, or omission on the part of the cloud computing service provider.

3-7-5 Notwithstanding the above, cloud computing service providers may:

3-7-5-1 Exclude or limit their liability for any indirect damage or lost revenue or profit, provided that this occurred unintentionally to the cloud computing subscriber;

3-7-5-2 Limit their liability to the maximum reasonable extent that may include, for example but is not limited to, other alternatives, and the sum of fees paid or owed by a cloud computing service subscriber under its contract with the cloud computing service subscriber and/or compensation of the cloud computing service subscriber through service credits;

3-7-5-3 Limit its liability in cases of cybersecurity incidents or breaches of cybersecurity - as long as this does not contradict what is issued by the National Cybersecurity Authority - if the subscriber chooses: (1) A "self-coverage solution", provided that the option was presented by the cloud computing service provider, or (2) To reduce backup capacity, or other solutions legally provided by the service provider to reduce cybersecurity risks.

3-7-6 Without restricting Article No. 3-7-5 and without contradicting what is issued by the National Cybersecurity Authority, the cloud computing service providers may exclude or limit their responsibilities towards non-individual cloud computing subscribers to the extent they agree with those subscribers under the cloud computing contract.

3-8 Quality Standards

3-8-1 The service providers registered with CITC shall:

3-8-1-1 Notify the cloud computing subscribers, upon request, of actual completion level for any requirements related to a service level agreement (if applicable) for the last twelve months or the period that has elapsed since the commencement of the cloud computing contract, whichever is the shortest.

3-8-1-2 Notify their service subscribers, upon request, of any authentication system or standards met by the service providers in relation to the relevant cloud computing services.

3-8-1-3 Adhere to any documentation plans and/or standards (including the encryption standards issued by the National Cybersecurity

Authority) that can be defined as mandatory by virtue of a decision from CITC regarding the type of the cloud computing service provided by the service provider.

3-8-1-4 Abide by any rules or guidelines approved by CITC in relation to business continuity, disaster recovery and risk management.

3-8-2 The encryption carried out by the cloud computing subscribers for their data or content must not affect the obligations of the cloud computing service provider under this Regulatory Framework.

3-8-3 CITC may, from time to time, issue decisions - without contradicting what is issued by the National Cybersecurity Authority - regarding mandatory or optional authentication plans and standards for cloud computing that may differ according to the required level of cybersecurity, the type of cloud computing service provider, the concerned computing subscriber, or other standards.

3-8-4 Without prejudice to any more specific requirement that may be required under Paragraph No. 3-8-3 above, the service providers registered with CITC in accordance with Article No. 2-3 above shall prove to CITC, at its discretion, when applying for registration that their "cloud services" will be of acceptable quality and sufficiently reliable through general standards based on the following:

3-8-4-1 Applicant resources dedicated to cloud computing.

3-8-4-2 Relevant experience.

3-8-4-3 Conformity with the applicant's technical standards, including the relevant standards set by CITC in the guidelines, manuals or practice behaviors, exceptional standards, or any other approved technical standards that exceed those established or equivalent standards according to CITC's absolute discretion.

3-9 Content Filtering

3-9-1 The cloud computing subscriber’s content or data in the cloud computing system, to which this Regulatory Framework applies, may be excluded from filtering the content according to a decision by CITC if the subscriber’s content or data:

3-9-1-1 cannot be accessed directly by any of the cloud computing users or Internet users in the Kingdom; or

3-9-1-2 can be accessed by cloud computing users only from: (1) private cloud computing, or (2) connectivity-bound communications networks between service providers and connections under the control of a cloud computing subscriber.

3-9-2 The provisions of Paragraph No. 3-9-1 shall be applied without prejudice to any other regulations or decisions issued by other competent authorities in the Kingdom, with regard to content filtering.

3-10 CITC Powers

3-10-1 Any breach of the provisions of this Regulatory Framework, or CITC's other regulations shall be subject to the penalties that may be imposed by CITC pursuant to its regulations without prejudice to any penalties that may be imposed under any other applicable laws and regulations in the Kingdom, including the Anti-Cyber Crime Law issued by Cabinet Resolution No. (79), 03/07/1428H, and approved by High Order No. (17/M), dated 03/08/1428H, and the Electronic Transactions Law issued by Cabinet Resolution No. (80), date 03/07/1428H, and approved by Royal Decree No. (18/M), dated 03/08/1428H, and any other provisions that may amend or replace it in the future.

3-10-2 The service provider registered with CITC shall provide CITC with any report or information requested within the requirements for the application of this document within the specified period and as stated in CITC's request, and it shall be responsible before CITC for any failure that results from that. In addition, CITC will treat these documents and information with complete confidentiality, according to its absolute discretion.

3-10-3 The service provider registered with CITC shall cooperate to the maximum extent with CITC's inspectors and facilitate their tasks and make available all possible resources of the service provider to carry out the inspection or audit or follow up on compliance, including: Reviewing the service provider's systems and providing the inspector with all the required documents that confirm the service provider's compliance with this Framework. CITC will treat these documents and information with complete confidentiality. CITC has the right to appoint an independent auditing body to carry out inspections, audits, and controls.

3-10-4 CITC has the right to issue guidelines, model cloud computing contracts, paragraphs, or recommendations or other texts with the aim to:

3-10-4-1 clarify any aspects of the current Regulatory Framework; and

3-10-4-2 Provide guidance to cloud service providers, cloud subscribers, and generally about any aspects of cloud computing.

3-10-4-3 supplement or amend this Regulatory Framework through mandatory or optional detailed executive decisions.

3-10-5 In the event that the service provider does not comply with the obligations contained in this document, CITC has the right to take legal actions against the service provider, including suspending or canceling the registration or any other procedure decided by CITC in accordance with its terms of reference.

3-11 General Provisions

3-11-1 Cloud computing service providers and cloud computing subscribers shall abide by the laws, regulations, controls, decisions, rules and policies issued by the competent authorities in the Kingdom, including - but not limited to - the National Cybersecurity Authority, the National Data Management Office, and the Saudi Authority for Intellectual Property.

3-11-2 Cloud computing service providers may not apply any laws or regulations or accommodate requests that may conflict with the laws or security requirements in force in the Kingdom without obtaining CITC's express written consent.