هيئة الاتصالات وتقنية المعلومات
Communications & Information Technology Commission

Cloud Computing

Regulatory Framework

The Communications and Information Technology Commission (CITC)

Version (3)

1 Introduction[1]

1-1 Pursuant to Article 3 of the Telecom Act (the Act'), the communications and information technology sector must be regulated to, among other objectives, 'ensure creation of favorable atmosphere to promote and encourage fair competition in all fields of communications and information technology.

1-2 Council of Ministers Resolution no. 133 dated 21/5/1424H confirmed that the powers of the Communications and Information Technology Commission (CITC) extend into information technology, requiring the Commission to: :

1-2-1 Implement the policies, plans and programs approved for the development of information technology and set out the appropriate procedures;

1-2-2 Propose regulations and their amendments related to information technology, and pursue approval of these regulations from the appropriate authorities;

1-2-3 Issue the necessary licenses in accordance with the terms and acts related to them.

1-3 Council of Ministers 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 Act and CITC's Statute in regulating the matters related to information technology, such as cloud computing.

1-4 The Information and Communications Technology (ICT) sector is undergoing rapid change. Adoption, by CITC, of the present Cloud Computing Regulatory Framework will generate benefits by encouraging Cloud Computing Services in the Kingdom and providing increased regulatory clarity.

[1] Note: This document is only an approximate translation. The Arabic version prevails.

2 Definitions

2-1 The terms and expressions defined in the Act and its Bylaw shall have the same meaning in this Regulatory Framework.

2-2 The following terms and expressions shall have the meaning assigned to them hereunder:

2-2-1 '**Cloud Computing**' shall mean the use of a scalable and elastic pool of shareable physical or virtual resources (such as servers, operating systems, networks, software, applications, and storage equipment) with self-service provisioning and administration on-demand .

2-2-2 '**Cloud Computing Services**' (or '**Cloud Services**') shall mean information and communications technology (ICT) services provided through Cloud Computing, which include, but are not limited to, the storage, transfer or processing of Subscriber's Content in a Cloud System. The mere storage and processing of Subscriber's information (such as the name, contact details or information on past transactions) by a Person who provides services to these customers other than Cloud Computing Services does not constitute a Cloud Computing Service. 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 subscriber 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 subscriber does not manage or control the platform and the underlying cloud infrastructure which includes the network, servers, operating systems, or storage. However, the subscriber 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**' ('**CSP**') shall mean any Person providing Cloud Services to the public either directly or indirectly, such as a Cloud Provider, Cloud Broker, Cloud Aggregator, reseller or agent of a Cloud Provider, whereby :

2-2-3-1 '**Cloud Provider**' shall mean any Person providing Cloud Services to the public (entity or individual) through Datacenters it owns and/or manages itself, in whole or in part .

2-2-3-2 '**Cloud Broker**' shall mean any Person that acts as an intermediary between one or more CSPs and Cloud Subscribers.

2-2-3-3 '**Cloud Aggregator**' shall mean a type of Cloud Broker that packages and integrates several Cloud Services into one or more composite services that it offers to Cloud Subscribers.

2-2-4 '**Cloud Subscriber**' shall mean any Person to which a CSP agrees to provide Cloud Services based on a Cloud Contract or other business relationship between the CSP and that Person.

2-2-5 '**Cloud User**' shall mean any individual person making use of a CSP's Cloud Services provided to a Cloud Subscriber, based on a relationship between

that Cloud Subscriber and the Cloud User. An individual person can be both a Cloud User and a Cloud Subscriber if the Cloud Contract is concluded for the provision of Cloud Computing Services to a single Cloud User".

2-2-6 '**Cloud Contract**' shall mean an agreement for the provision of Cloud Services, concluded between a CSP and a Cloud Subscriber.

2-2-7 '**Cloud Computing System**' shall mean an electronic information system comprising hardware, software and networking elements that are owned, controlled, operated, leased or otherwise relied on by a CSP to supply Cloud Services to Cloud Subscriber. A Cloud System may comprise one or more Datacenters, among other elements.

2-2-8 '**Public Cloud**' shall mean a Cloud System provisioned for open use by the public.

2-2-9 '**Community Cloud**' shall be a Cloud System provisioned for the exclusive use of a closed group of Cloud Subscribers sharing certain social, business, administrative or other objectives.

2-2-10 '**Private Cloud**' shall mean a Cloud System provisioned for the exclusive use of a single Cloud subscriber.

2-2-11 '**Hybrid Cloud**' shall mean a combination of two or more Cloud Systems (Private, Public and/or Community Clouds) that are bound together by standardized or proprietary technology that enables data and application portability.

2-2-12 '**Datacenter**' shall mean a facility consisting of computing infrastructure and supporting components, which are housed in the same location and used, at least in part, for the storage and/or processing of subscriber's Content and subscriber's Data.

2-2-13 '**Content**' shall mean any software, text, files, audio, video, images, graphics, animations, illustrations, information, personal, business or other data, in any format.

2-2-14 '**Subscriber Content**' shall mean any Content provided or generated by a Cloud subscriber that is stored or processed in a Cloud System pursuant to a Cloud Contract for the provision of Cloud Services through that Cloud System to that Cloud subscriber.

2-2-15 '**Subscriber Data**' shall mean any data falling under at least one of the following categories, insofar as that data are, or have been, part of the

Subscriber Content or are, or have been, generated by the CSP with regard to one or more of its Cloud Subscriber or Cloud Users .

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 allow the user to be identified by.

2-2-15-2 Any data relating to a Cloud Subscriber's business activities, business information or financial affairs. Such data can include, for example, the Cloud Subscriber's prices, data on its personnel, product or client lists, its financial, audit and security data, and its business and product development data, even if such data or other information are in the public domain.

2-2-15-3 Any data generated by, or for, the CSP concerning the Cloud Subscriber's activity log, billing, usage volume, statistics or other Cloud Subscriber-specific information associated with its use of the Cloud Services offered by the CSP.

2-2-16 '**Subscriber Address**' shall mean a Cloud Subscriber's (i) address provided in the Cloud Contract or (ii) invoicing address, and if the two are different and only one of them is in the KSA, Subscriber Address shall mean that address.

2-2-17 '**Third Party Content**' shall mean any Content, in electronic form, obtained or derived from any Person other than the CSP or the Cloud Subscriber and made available to the Cloud Subscriber through, or in conjunction with, the Cloud Subscriber's use of the Cloud Services. Such Content can include, without limitation, data, information, software, documents, images, audio or video.

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

2-2-19 '**Intellectual Property Violating Content**' means a subscriber or third-party content that infringes intellectual property rights.

2-2-20 '**Residence**' shall mean a permanent or temporary residence in the Kingdom under the Kingdom's laws. It shall not include a temporary presence of Persons on a short visit or transiting through the Kingdom.

2-2-21 '**Service Credits**' shall mean compensation mechanisms offered by a CSP to a Cloud Subscriber if the CSP's actual performance fails to meet the

standards that are set in the Cloud Contract or are otherwise required under this Regulatory Framework. Examples of Service Credits can include discounts on current or future bills, and time of Cloud Services added at the end of a billing cycle free of charge.

2-2-22 '**Service Level Agreement**' shall mean an agreement between a CSP and a Cloud Subscriber that defines the quality of the Cloud Services to be delivered to that Cloud Subscriber in terms of a set of measurable properties specific to Cloud Computing.

3 The Regulatory Framework

3-1 Scope

3-1-1 The provisions of this Regulatory Framework shall apply with regard to any Cloud Service provided to Cloud Subscribers having a Residence or Subscriber 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 Article 3-3-12 (Reporting major cybersecurity incidents) below.

3-1-2-2 Articles 3-5-4 and 3-5-5 (Remove law-violating content, or Intellectual Property violating content, at the request of CITC or any other competent authority) and Article 3-5-6 below about (Notifying CITC of violations of Anti-Cyber Crime Law).

3-1-2-3 The exception referred to in Article 3-4-3-1 below.

3-1-2-4 Article 3-2 (Registration to provide cloud computing services) below.

3-1-3 Any obligations arising from Article 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 fully registering with CITC; provided that it uses the communications infrastructure, including international communications, through those licensed 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 Article 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 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 Article 3-3-4.

Table 1: Subscriber Data Classification

Subscriber Data Classification	Classification Level	Description
	Top Secret	Data shall be classified as "Top Secret", if unauthorized access to or disclosure of such data or its content adversely and exceptionally affects in a way that is difficult to resolve:

Saudi Government Data		• National interest including violations of conventions and treaties, adverse damage to the reputation of the country, diplomatic relations and political affiliations, operational efficiency of the security or intelligence operations of military forces, national economy, national infrastructure and Government functions, and/or • The Kingdom's government entities functionality causing damage to the national interest, and/or • Individuals' health and safety at massive scale and privacy of Protected Individual personnel, and/or • Catastrophic damage to the environment or natural resources
	Secret	Data shall be classified as "Secret", if unauthorized access to or disclosure of such data or its content adversely affects: • Affects national interest such as damage to the reputation of the country, diplomatic relations, operational efficiency of the security or intelligence operations of military forces, national economy, national infrastructure, Government functions, or the investigation of major cases such as terrorism funding and/or • Financial loss that leads to bankruptcy or inability of organizations to perform their duties or major loss of competitive abilities or combination thereof, and/or • Causes significant harm or injury impacting life of individuals • Causes long-term damage to the environment or natural resources
	Confidential	Data shall be classified as "Confidential" data, if unauthorized access to or disclosure of such data or its content causes: • Contained negative affect on the Kingdom's government entities' operations, the Kingdom's economy, and/or • Damage to any entity's assets and limited loss to its financial and competitive status, and/or • Negative effect on individual's interests • Contained damage in the short-term to the environment or natural resources.
	Public	Data shall be classified as "Public", if unauthorized access to or disclosure of such data or its content has no impact on: • National Interest, or • Organizations, or • Individuals, or • Enviroment
Non-Government Data	**Data Received from Saudi Government Entities**: 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: Cloud Providers Registeration Classes

Service Provider Registration Classes[3] / Data Classification		(A)	(B)	(C)[2]
Saudi Government Data	Top Secret			✓
	Secret			
	Confidential		✓	✓
	Public	✓	✓	✓
Non-Government Data	Data Received from Saudi Government Entities	Classified as received from the government agencies		
	Other Data	✓	✓	✓

3-3-2 The provisions of this Regulatory Framework shall be without prejudice to any applicable law, regulation, guideline, code of conduct, internal instruction, corporate policy or any other legal, regulatory, administrative or corporate rule, concerning:

[2] To deal with government agencies' data that are classified as Secret and Top Secret, 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] Note: The service provider registration classes is the class 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, published on CITC's website, explains the special requirements for each class.

3-3-2-1 The Cloud Subscribers' right, if any, to outsource, transmit, process or store in a Cloud System Subscriber Content or any data or information.

3-3-2-2 The Cloud Subscribers' obligation to ensure that, if allowed, any such outsourcing, transmission, processing or storage should be subject to certain cybersecurtiy or data protection restrictions or safeguards, in addition to those specified to 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 Article 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 Article 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 (Saudi Government Data) 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 class 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 Article 3-3-1.

Subscriber Content Location and Transfer

3-3-7 CSPs must inform any Cloud Subscriber, upon his request, of the cybersecurity features offered by the CSP or applied to the Cloud Subscriber's Content. CSPs may also satisfy this obligation by making such information available in online format for Cloud Subscribers.

3-3-8 The cloud computing service providers registered with CITC and cloud computing subscribers shall not transfer any content from the Saudi Government Data 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 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 3-2 above.

3-3-10 Without prejudice to their obligations stipulated in Article 3-3-7, CSPs registred with CITC must inform their Cloud Subscribers in advance whether their Subscribers' Content will be transferred, stored or processed outside the Kingdom, permanently or temporarily.

Reporting Cybersecurity Incidents

3-3-11 CSPs must inform Cloud Subscribers, without undue delay, of any cybersecurity breach or information and data leakage that those CSPs become aware of, if such breach or leakage affects, or is likely to affect, those Cloud Subscribers' Cloud Content, Subscriber Data or any Cloud Service they receive from that CSP.

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 Subscriber's content from Saudi Government Data.

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 CSPs must inform their Cloud Subscribers of any insurance coverage that those CSPs have for any civil liability to those Cloud Subscribers. This information to the Cloud Subscribers must include at least the essential features of the CSP's insurance coverage, if these are reasonably required

for Cloud Subscribers to assess their exposure to risk and decide on their own insurance coverage accordingly.

3-3-14 Cloud Providers must adopt internal rules and policies on business continuity, disaster recovery and risk management, and provide to their Cloud Subscribers or the CSPs they co-operate with, upon their request, a summary of these rules and policies.

3-4 Subscriber Data Protection

3-4-1 The provisions of this Article 3-4 shall be binding upon CSPs 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, although not a party to such a Cloud Contract with the Cloud Subscriber concerned, alone or jointly with others determine the purposes and means of the processing of the relevant Cloud Subscriber's Data in a Cloud System.

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 another party to provide to any third party (including, but not limited to, any individuals, legal entities, domestic or foreign government or public authorities) subscriber Content or subscriber Data.

3-4-2-2 Process or use subscriber Content or subscriber Data for purposes other than those allowed under the Cloud Computing Agreement with the Cloud subscriber concerned. The service provider must disclose (on a detailed separate document) any capabilities they have to view any data stored within their possession, in the Kingdom, or that have been processed or transferred in or through it, or to decipher that data, or to assist any third party or allow that party to view the data or decipher it. The service provider shall not to implement any new capabilities in this regard without obtaining an explicit written approval from CITC.

3-4-3 A CSP's obligations under Article 3-4-2, above, shall not apply with regard to any subscriber Content or subscriber Data that meets one of the following two conditions :

3-4-3-1 The CSP is required to disclose, transmit, process or use that subscriber Content or subscriber Data under the laws of the Kingdom;, or

3-4-3-2 The subscriber's data (non-governmental entities) is of type Other Data, and the relevant Cloud Customer provides its express prior consent (whether in an 'opt-in' or an 'opt-out' form), which the Cloud Customer shall remain free to withdraw at any time in the future.

3-4-4 CSPs shall grant Cloud subscribers the right and the technical capability to access, verify, correct or delete their subscriber Data in a manner that does not contradict with what is issued by the National Data Management Office regarding personal data.

3-4-5 The CSPs' obligations under Article 3-4-4, above, shall be without prejudice to the CSPs' right to the subscriber Data mentioned in Article 2-2-15-3, above, if and for 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 CSPs in accordance with any of the laws in force in the Kingdom.

3-4-6 The provisions of Article 3-4 shall be without prejudice to any applicable legal, regulatory or contractual provision conferring a higher degree of protection, and associated rights and obligations, with regard to any categories of personal or business data that form part of subscriber Data or subscriber Content covered by this Regulatory Framework.

3-5 Law-Violating Content and Intellectual Property

3-5-1 The provisions of Article 3-5 shall be binding upon CSPs who:

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

3-5-1-2 those who, although not a party to such a Cloud Contract with the Cloud subscriber concerned, alone or jointly with others exercise control over the processing of the relevant subscriber Content.

3-5-2 Subject to the provisions of this Article 3-5, a CSP shall not incur any administrative or criminal liability under this Regulatory Framework or any law, regulation, resolution, or instruction, including the Anti-Cyber Crime Law, based only on the fact that a content that violates the law, or infringes the intellectual property rights of others has been uploaded, processed or stored on the CSP's Cloud System.

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 law-violating content, or subscriber's content that infringes any intellectual property rights of others.

3-5-4 If CITC or any other authorized entity in the Kingdom orders in writing the CSP to remove any law-violating content or content that infringes any intellectual property rights of others from a Datacenter or other element of a Cloud System located in the Kingdom that is used or relied on by the CSP for the provision of Cloud Services under the scope of Articles 3-1-1 and 3-1-2, above, the CSP shall be responsible for ensuring that such law-violating content or content that infringes any intellectual property rights of others is:

3-5-4-1 removed from the Datacenter or other element of the Cloud System located in the Kingdom; or

3-5-4-2 is rendered inaccessible in the Kingdom and/or (if this is required under the Kingdom's international obligations) any other jurisdiction.

3-5-5 CSPs may, at their own initiative or following a third party request, remove from their Cloud System or render inaccessible in the Kingdom and/or in any other jurisdiction any law-violating content or content that infringes any intellectual property rights of others, provided that:

3-5-5-1 this is in accordance with the provisions of the Cloud Contract, and

3-5-5-2 the CSP provides adequate notice to the affected Cloud subscriber.

3-5-6 CSPs must notify CITC and/or any other authorized entity, without undue delay, if they become aware of the presence of any Subscriber Content or other information on their Cloud System that may constitute a violation of rules and regulations in the Kingdom.

3-5-7 CSPs must refer any third parties complaining against law-violating content or content that infringes any intellectual property rights of others on their Cloud System to the competent authorities in the Kingdom, unless they decide to address that complaint directly under the provisions of Article 3-5-5, above.

3-5-8 CSPs may inform a Cloud Customer that law-violating content or content that infringes any intellectual property rights of others found in his Subscriber Content has been taken down unless CITC or any other

authorized entity prevents the CSP from doing so. CITC and/or any other authorized entity shall not unreasonably refuse allowing a CSP to do so, particularly if a failure of the CSPs to inform the Cloud Subscriber about the taking down of its Cloud Content threatens to create any liability of the CSP.

3-5-9 The provisions of Article 3-5 shall be without prejudice to the CSPs' obligation to co-operate with the Kingdom's authorities, pursuant to any applicable law or any commitments undertaken in their registration, in law enforcement matters associated with law-violating content or content that infringes any intellectual property rights of others.

3-5-10 CSPs must grant their Cloud Subscribers all necessary and lawful intellectual property licenses for the use of any software or other legally protected intellectual work in the Cloud Services provided under their Cloud Contract, commensurate to the duration (if applicable) and scope of the Cloud Contract.

3-6 Information About Cloud Computing Service Contracts and the Mandatory Minimum Content

3-6-1 Prior to the conclusion of a Cloud Contract with a Cloud Subscriber, CSPs must provide clear and transparent information to that Cloud Subscriber on the object of the service, the conditions of use, Cloud Service levels, and applicable payment terms and mechanisims, and the class in which the CSP 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 Article 3-3-1.

3-6-2 The above obligation shall be without prejudice to any other additional information that CSPs may need to communicate to Cloud Subscribers if so required under their registration or other applicable rules.

3-6-3 Without prejudice to any other obligation under this Regulatory Framework, CSPs must ensure that at least the following information is incorporated in their Cloud Contracts:

3-6-3-1 Identification of the CSP and its profile, business address and full contact details.

3-6-3-2 A description, and allowed use of the services to be provided.

3-6-3-3 Cloud Contract duration (if any applies), applicable charges, payment terms and termination.

3-6-3-4 Rules on handling of Subscriber Content, including its processing and processes to enable Subscriber Content to be retrieved by the Cloud Subscriber upon the Cloud Contract's termination.

3-6-3-5 Information on the availability, terms and conditions of any Service Level Agreement (SLA) that may be offered by the CSP.

3-6-3-6 A procedure on how to deal with and resolve Cloud Subscriber complaints.

3-6-3-7 Applicable law for the interpretation of the Cloud Contract and the resolution of any disputes, it being understood that, if this is other than the law of the Kingdom, it may not override any of the provisions of this Regulatory Framework or any other mandatory rules of the Kingdom that may not be overridden through choice of law provisions.

3-6-4 CSPs must provide a Cloud Subscriber care service for the resolution of any Cloud Subscriber complaint. Such service shall be without prejudice to, any other legal remedy and dispute resolution procedure available under applicable laws, also including this Regulatory Framework.

3-6-5 Cloud Subscribers and CSPs shall have a right to refer their disputes, jointly or separately, to any dispute resolution procedure available before CITC pursuant to its Statutes, without prejudice to any other, non-exclusive, alternative dispute resolution procedures or choice of law clauses that may be allowed under applicable law.

3-6-6 Upon termination of the Cloud Contract with a Cloud Subscriber, and if the Cloud Subscriber so requests, the CSP must:

3-6-6-1 Provide to the Cloud Subscriber a copy of the Cloud Subscriber's Cloud Content stored on the CSP's Cloud System at the time of the Cloud Contract's termination, in a commonly used format, or

3-6-6-2 Allow and offer the Cloud Subscriber the means to download and/or retrieve such Cloud Content, in a commonly used format.

3-6-7 As an alternative to the options of Articles 3-6-6-1 and 3-6-6-2 above, the CSP may transfer the Cloud Subscriber's Cloud Content, in a suitable format, directly to another CSP of the Cloud Subscriber's choice, where this is technically feasible.

3-7 Subscriber Protection and Unfair Contract Terms

3-7-1 CSPs shall bear responsibility before CITC and its individual subscribers for any act or omission by the CSP, its agents, subcontractors or employees (acting within the framework of their agency, employment, or subcontracting relationship with the CSP), incurring liability to such Cloud subscribers under this Article 3-7 or any other applicable laws of the Kingdom, regardless of whether such acts or omissions take place in the Kingdom or abroad.

3-7-2 CSPs may not contractually exclude their liability to their individual Cloud Subscribers for the losses or damages listed below, if these may be reasonably attributed, in whole or in part, to intentional or negligent acts or omissions of those CSPs:

3-7-2-1 Any loss of, or damage to, Subscriber Content or Data, if this is linked to the CSP's processing of, or other interaction with, such Subscriber Content or Data.

3-7-2-2 Quality, performance, accessibility, downtime or other similar service parameters that do not conform with the CSP's obligations under its Cloud Contract with the Cloud Subscriber concerned or with the provisions of any mandatory legal provisions; and

3-7-2-3 Any cybersecurity incidents.

3-7-3 A 'best efforts' clause by a CSP in a Cloud Contract may not exclude its liability to individual Cloud Subscribers for acts or omissions committed intentionally or through gross negligence.

3-7-4 Cloud Subscribers shall bear the burden of proof that any loss or damage referred to in Articles 3-7-1 and 3-7-2 above is reasonably attributed, in whole or in part, to intentional or negligent act or omissions of the CSP.

3-7-5 Notwithstanding the above, CSPs may:

3-7-5-1 Exclude or limit their liability for any indirect damage or any loss of revenue or profits, provided that this is caused nonintentionally to a Cloud Subscriber;

3-7-5-2 limit their liability by a reasonable maximum amount, which may include, among other alternatives, a function of the fees paid or due by the Cloud Subscriber under his Cloud Contract with the CSP and/or compensate the Cloud Subscriber through Service Credits;

3-7-5-3 in the case of liability for cybersecurity incidents or breaches of cybersecurity, limit their liability - as long as this does not contradict with what is issued by the National Cybersecurity Authority - if the Cloud Subscriber (i) opts for an 'own coverage' solution, provided that such an option is offered by the CSP, or (ii) declines the redundancy or other solutions lawfully offered by the CSP to reduce cybersecurity risks.

3-7-6 Without restricting Article 3-7-5 and without contradicting with what is issued by the National Cybersecurity Authority, CSPs 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 CSPs registered with CITC shall:

3-8-1-1 Inform their Cloud Subscribers, upon request, of the actual levels of achievement of any SLA requirements (if applicable) for the last 12 months or the period since the start of the Cloud Contract, whichever is shorter;

3-8-1-2 Inform their Cloud Subscribers, upon request, of any certification systems or standards that these CSPs meet with regard to their Cloud Services to the relevant Cloud Subscriber;

3-8-1-3 Comply with any certification schemes 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 with regards to the type of Cloud Services provided by that CSP;

3-8-1-4 Comply with any rules or guidelines adopted by CITC with regards 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 shall not affect the CSPs' obligations under this Regulatory Framework.

3-8-3 CITC may issue, from time to time - as long as this does not contradict with what is issued by the National Cybersecurity Authority -, decisions on mandatory or voluntary certification schemes and standards for Cloud Computing, which may vary depending on the required level of

cybersecurity, the type of CSP or Cloud Subscriber concerned, or by other criteria.

3-8-4 Without prejudice to any more specific requirement that may be required under Article 3-8-3 above, CSPs, subject to a registration under Article 3-2 above, must demonstrate to CITC's satisfaction, when applying for registration, that their Cloud Services will be of an acceptable quality and sufficiently secure by general industry standards, based on:

3-8-4-1 The applicant's resources dedicated to Cloud Computing;

3-8-4-2 The applicant's relevant experience, and

3-8-4-3 The technical standards complied with by that applicant including the standards listed by CITC as relevant in Guidelines, Guides or Codes of Practice or, exceptionally, any other technical standards that are demonstrably equivalent or superior to those standards, to CITC's satisfaction.

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 according to a decision by CITC if the subscriber's content or data:

3-9-1-1 is not directly accessible by any Cloud Users or Internet users in the Kingdom; or

3-9-1-2 is accessible only to Cloud Users of (i) a Private Cloud or (ii) a specific communications network limited to connections between a CSP and connections under the control of a single Cloud Subscriber.

3-9-2 The provisions of Article 3-9-1 shall be applied without prejudice to any other regulations or decisions issued by other competent authorities in the Kingdom, with regards to content filtering.

3-10 CITC Powers

3-10-1 Any violation of the provisions of this Regulatory Framework shall be subject to the penalties that CITC may impose under its Statutes, without prejudice to any penalties that may be imposed under any other applicable law in the Kingdom. Such other applicable law includes, in particular: the Anti-Cyber Crime Law (issued under the Council of Ministers Decision No. 79, dated 7/3/1428H, and approved by Royal Decree No. M/17, dated

8/3/1428H) and the Electronic Transactions Law (issued under the Council of Ministers Decision No. 80 dated 7/3/1428H and approved by Royal Decree No. M/18 dated of 8/3/1428H), and any provisions that may amend or replace them in the future.

3-10-2 CSP 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 may issue guidelines, model Cloud Computing contracts or clauses, guides, recommendations or other texts aimed at:

3-10-4-1 clarifying any aspect of the present Regulatory Framework;

3-10-4-2 providing guidance to CSPs, Cloud Subscribers and the public in general on any aspect of Cloud Computing;

3-10-4-3 Complementing this Regulatory Framework through mandatory or voluntary detailed implementation provisions.

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 revoking the registration or any other procedure decided by CITC in accordance with its terms of mandate.

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 explicit written consent.

هيئة الاتصالات وتقنية المعلومات
Communications & Information Technology Commission