هيئة الاتصالات وتقنية المعلومات
Communications and Information Technology Commission

Public Consultation Document on the Proposed Regulation for Cloud Computing

Issued by CITC on July 2016

Table of Contents

1 Introduction

1.1 Pursuant to the Telecommunications Act, the Bylaw and the Ordinance, the Communications and Information Technology Commission ('CITC') is authorized to regulate the Information and Communications Technology ('ICT') sector in the Kingdom of Saudi Arabia ('KSA').

1.2 Pursuing its goal of creating a favourable environment to foster the provision and development of cloud computing services in the KSA, CITC is in the process of reviewing the existing regulations affecting cloud computing and the need for any cloud-specific provisions.

1.3 CITC invites all stakeholders and members of the public, including private individuals, public organizations and commercial entities (together, the Respondents) to participate in this Public Consultation process relating to the regulation of cloud computing in the Kingdom.

2 Scope and Objectives of the Public Consultation

2.1 This public consultation is being issued in order to seek comments from all stakeholders and interested members of the public on the need for a regulation of cloud computing in the Kingdom and the draft versions of the following documents that, together, form such a proposed regulation:

- Draft Regulatory Framework on Cloud Computing (Annex A)
- Draft Application Procedure (Annex B)
- Draft Cloud Infrastructure and Services License (CISL) (Annex C)
- Draft Cloud Services License (CSL) (Annex D)
- Draft Cloud Services Declaration (Annex E)

3 Providing Comments on the Consultation Documents

3.1 These Public Consultation Documents, including their annexes, are available on CITC's website at (**www.citc.gov.sa**).

3.2 Respondents who wish to express opinions on the Public Consultation Documents are invited to submit their comments in writing to CITC. All comments must be received by CITC no later than **17/12/1437H**, corresponding **to18/9/2016**.

3.3 Comments filed in relation to this Public Consultation must be submitted to one of the following addresses:

- E-mail to: [cloud_computing@citc.gov.sa]

- Delivery by hand or by courier to:

Communications and Information Technology Commission (CITC)

Corner Prince Turki Ibn Abdulaziz Al Awwal Road and Al Imam Saud Ibn

Abdulaziz Road

P.O. Box 75606

Riyadh 11588

Kingdom of Saudi Arabia

3.4 CITC invites comments and responses to the specific numbered questions set out in this Public Consultation Document. CITC encourages respondents to support their comments with a relevant justification and analysis, data and information based on the current situation or on their relevant experience in other countries.

3.5 In their comments, respondents are requested to indicate the question number and the annex to which each comment relates.

3.6 CITC is under no obligation to adopt the comments of any respondent and it does not intend to publish the responses it receives to this consultation.

4 Background

4.1 'Cloud Computing Services' (or 'Cloud Services') refer to information and communications technology (ICT) services provided through Cloud Computing, which involve the storage, transfer or processing of User Content in a Cloud System. The mere storage and processing of customer 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.

4.2 The term 'cloud computing' generally refers to a paradigm for enabling network access, through the 'cloud' (essentially, the Internet), to a scalable and elastic pool of physical or virtual resources (such as servers, operating systems, networks, software, applications, and storage equipment) that can be shared with other users, while at the same time allowing each user to benefit from self-service provisioning and administration on-demand.

4.3 There is growing demand for cloud computing solutions in the KSA from both the public and the private sector. Key drivers of the adoption of cloud services are reported to be cost savings, scalability and efficiency gains.[1] Cloud services are, in general, more cost effective than other types of ICT services or solutions, because they rely on the outsourcing of infrastructure, software and other IT resources to 'cloud service providers' (CSPs) that can achieve greater economies of scale by managing the IT systems of several clients.

4.4 CITC believes the development of a strong local cloud services industry, which offers state-of-the-art and cost-efficient services to businesses and individuals in the Kingdom and abroad, has the potential to make a major contribution to the realization of the Kingdom's Vision 2030. Creating a developed digital infrastructure, in which cloud computing is an essential component, is recognized by the Vision to be "integral to today's advanced industrial activities" as it "attracts investors and enhances the fundamental competitiveness of the Saudi economy".

1 ICT Report on "Datacenter, Managed and Cloud Services in Saudi Arabia": http://www.citc.gov.sa/English/Reportsandstudies/Reports/Documents/ICTDatacenter_en.pdf.

5 The need for regulation

5.1 There is no single 'cloud-specific' law or regulation in the KSA, but rather a number of more general laws and regulations with a potential impact on cloud computing, such as:

- The **Telecommunications Act**, whose Art. 2 vests CITC with supervisory powers for the telecommunications sector, based on its more specific functions and duties conferred upon it by this Act, the Telecommunications Bylaws and the CITC Ordinance.

- Further, Articles 37 and 38 of the Telecommunications Act sanction, among other prohibited acts, the interception of any data carried on public telecommunications networks and the intentional disclosure of intercepted information or contents (unless in the course of duty).

- **Council of Ministers Resolution no 133 of 21/5/1424**H, which has expressly expanded CITC's regulatory powers into the information technology field.

- The **Telecommunications Bylaw**, particularly as regards to licensing requirements for the providers of electronic communications services and networks (Chapter 2) and protection and prevention against intrusion (Chapter 13).

- The **Electronic Transactions Law of 1428H/2007**, which regulates matters concerning electronic transactions and signatures.

- The **Anti-Cyber Crime Law of 1428H/2007**, which defines a series of cyber crimes and related penalties.

- Council of Ministers decision number 81 issued in 1430H regarding the use of computers and information networks in government agencies: "Government agencies and administrations are required to host their internet websites at their networks, at other government agencies networks or through providers with a license issued by CITC. The hosting infrastructure must be in KSA and the hosting contracts must contain information confidentiality protection terms".

5.2 Despite these laws and regulations, the industry has raised concerns over the current uncertainty regarding the regulatory status of cloud computing, the need for registration or licenses, the applicable information security and data protection rules, and the rights and obligations of each party. These views coincide with the findings from the international benchmarking carried out recently by CITC. More generally, security risks in connection with cloud usage seem to be an important concern for both CSPs and users.

5.3 Therefore, CITC believes that it is appropriate to develop cloud-specific regulations that will benefit both the industry and the users, with the following objectives:

- Providing clarity and regulatory certainty on the rights and obligations of the providers and users of cloud computing services.
- Establishing a clear regulatory basis to manage potential security risks connected with the use of cloud services.
- Encouraging improved quality of cloud services.
- Encouraging investment in a local cloud industry.

5.4 The remainder of this document presents the proposed regulatory structure and its detailed provisions.

Question 1: What are your views on the above stated objectives? Do you think cloud-specific rules addressing these objectives would benefit the industry and users of cloud services? Are there any other objectives you would find beneficial? If so, please state them, providing, if possible, supporting evidence for your statement.

6 Proposed Regulatory Scheme

6.1 The services and business models covered by cloud computing are very broad and always changing. Cloud regulations must therefore be as flexible and encompassing as possible.

6.2 CITC is of the view that cloud computing regulation should therefore combine a number of regulatory instruments, including:

6.2.1 A general 'Regulatory Framework on Cloud Computing' defining the general rules and regulations applicable to the cloud computing industry in the Kingdom - see Section 7.

6.2.2 A licensing scheme that clearly indicates the cases in which CSPs should obtain any license, including any associated provisions, benefits, obligations and rules - see Section 8.

6.2.3 Additional documents on more detailed topics, some of which may be issued by CITC in the future to support the Regulatory Framework, such as guidelines, model agreements/standard clauses, codes of conduct and guides.

7 Regulatory Framework on Cloud Computing

7.1 Definitions

7.1.1 The proposed Regulatory Framework contains definitions of cloud computing services and associated terms, including a distinction between different categories of market players (see Annex A, Article 2).

Question 2: What are your views on the definitions included in Article 2 of the Draft Regulatory Framework on Cloud Computing? If you believe that there are any further terms that should be defined in the Regulatory Framework, please mention them and the reasons for their inclusion.

7.2 Scope of the Regulatory Framework

7.2.1 In principle, the Regulatory Framework will apply to cloud computing services provided within the Kingdom, irrespective of the location of the physical servers or datacentres from which such services are provided or the jurisdiction under which the provider operates.

7.2.2 Additionally, some provisions of the Regulatory Framework will be applicable to the provision of cloud computing services from infrastructure located in the territory of the KSA, even if the cloud user is resident or has a cloud user address abroad.

7.2.3 The Draft Regulatory Framework on Cloud Computing in Annex A defines, in Article 3.1, the scope of its applicability.

Question 3: What are your views on the proposed scope of the Regulatory Framework regarding, for example, services covered and geographical reach?

7.3 Licensing requirements

7.3.1 CITC believes that licenses can represent a useful regulatory mechanism to eliminate any uncertainty about the applicable rules, and facilitate the CITC's supervision of those CSPs providing cloud services considered to be of critical importance.

7.3.2 However, not all services provided within the cloud computing environment, nor all types of CSP, justify the same licensing requirements. Examples of factors that, in CITC's view, influence the need for licensing requirements include whether the CSP has control over critical infrastructure, the extent to which a CSP interacts directly with users and controls their data, the information security level required for the data controlled by the CSP and the scale of its commercial presence in the KSA.

7.3.3 Based on this reasoning, CITC proposes a three-category licensing scheme:

- CSPs operating under a 'Cloud Infrastructure and Services License' (CISL). These will include CSPs with datacentres or other key cloud infrastructure in the KSA, and those processing or storing sensitive user content (i.e., 'Level 3' user content, as defined in Article 3.3 of the Regulatory Framework).

- Other CSPs, operating under a 'Cloud Services License' (CSL) or a simple registration (an alternative being considered by CITC) based on a declaration from the CSP concerned.

- CSPs having only a limited commercial presence in the KSA in terms of subscriber numbers and revenues will not require a license or registration.

7.3.4 The license categories would have implications for the information security levels of any user content that the licensee is allowed to process, as shown in the table below (please see section 7.4 regarding security levels):

Security Level	CSP License		
	CISL	CSL	None
Level 1	√	√	√
Level 2	√	√	
Level 3	√		

7.3.5 Regardless of the choice between these three alternatives, all CSPs will be required to comply with the provisions of the Regulatory Framework regarding their services provided in the Kingdom.

7.3.6 Article 3.2 of the Draft Regulatory Framework (Annex A) describes the licensing requirements for CSPs in line with the above criteria. It should be read in conjunction with article 3.3 for a better understanding of the relationship between licensing obligations and categories of user content.

Question 4: What are your views on the licensing/registration requirements set out in the Draft Regulatory Framework?

Question 5: What is your preference between a CSL or a registration requirement for CSPs falling under the second of the proposed three categories of CSPs?

7.4 Information security

7.4.1 The Regulatory Framework aims to clarify the basic applicable regulations covering information security for the cloud computing industry, including:

- Classification of data for information security purposes into a number of security levels, as presented in the following table:

Security Level	Categories of data	
	Owner	**Type**
Level 1	Individuals	Non-sensitive
	Private sector	Public/non-sensitive
Level 2	Individuals	Sensitive
	Private sector	Private but non-sensitive
	Public sector	Public/non-sensitive
Level 3	Private sector	Sensitive
	Private sector	Subject to sector-specific rules
	Public sector	Private (no public)
	Any	Set as Level 3 by user
Level 4	Public sector	National secrets

- Responsibility for classifying the information under the appropriate security level referred to in the previous paragraph.

- The limitations and regulations applicable to the transfer and storage or processing of user content outside the Kingdom.

- The CSP's reporting obligations in case of security breaches.

Question 6: What are your views on the data classification for information security purposes defined in the Draft Regulatory Framework and the specific provisions regarding information security (article 3.3)?

7.5 Protection of user data

7.5.1 The Regulatory Framework incorporates a number of basic provisions regarding data protection, including:

- Applicable restrictions for CSPs to provide, or allow another party to provide, cloud content or user data to third parties.

- Cloud users' right to access, verify and/or delete their user data.

7.5.2 CITC proposes to define 'user data' in this context more broadly than personal data, in order to also include cloud user's sensitive business information.

Question 7: What are your views on the provisions included in the Draft Regulatory Framework regarding data protection (article 3.4)?

7.6 User content regulations (unlawful content and intellectual property rights)

7.6.1 The Regulatory Framework defines the liabilities and obligations of each party if unlawful content or content that infringes intellectual property rights (IPR) is uploaded, processed or stored on a CSP's cloud system.

7.6.2 CITC is of the view that CSPs should have no obligation to actively monitor their users' content in order to detect and remove or restrict, as may be necessary, content of an unlawful or IPR-infringing nature, but should nonetheless have an obligation to:

- Remove or render inaccessible in the Kingdom such unlawful or IPR-infringing content, if ordered to do so by CITC or any other competent public authority of the Kingdom.

- Notify the Saudi authorities if they become aware of the presence of unlawful content that represents a violation of the Anti-Cybercrime Law.

- Relay to the Saudi authorities any complaints received by third parties about allegedly unlawful content.

7.6.3 To encourage self-regulation of the cloud industry, the Regulatory Framework gives CSPs the right to take down illicit content on their own initiative, or upon request by a third party.

7.6.4 Finally, CSPs should grant their cloud users all necessary and lawful licenses for the use of any software or other legally protected intellectual property used in the cloud services provided.

Question 8: What are your views on the provisions included in the Draft Regulatory Framework regarding unlawful content and intellectual property (section 3.5)?

7.7 Cloud contracts and consumer protection

7.7.1 CITC believes that it is appropriate for the Regulatory Framework to include a minimal set of requirements, which contracts between CSPs and their cloud users should address, namely:

- The contracts' minimum mandatory content and information.
- The right of CSPs to limit or exclude certain liabilities (or not).
- The obligation of CSPs obligation to provide customer care for the resolution of customer complaints.
- Provisions regarding the cloud contract's termination.

Question 9: What are your views on the proposed Regulatory Framework's provisions on cloud contracts and consumer protection (sections 3.6 and 3.7)?

7.8 Quality and industry standards

7.8.1 Industry standards for cloud computing remain a work in progress. It is common practice for CSPs to obtain certifications and comply with standards regarding their infrastructures and processes, but this is usually done on a voluntary basis to strengthen the CSPs' credentials on the market.

7.8.2 Given the current state of development of industrial standards for the cloud, CITC's view is that the Regulatory Framework should limit itself to provisions that aim to (a) provide some transparency to cloud users about the certifications in place and (b) allow CITC to provide, in the future

and if market circumstances require it, further guidance or rules on any required or applicable industry standards.

Question 10: What are your views on the proposed Regulatory Framework's provisions on quality and industry standards (section 3.8)?

7.9 Content Regulation

7.9.1 The Regulatory Framework clarifies how content regulation should apply to cloud computing services. In principle, the Regulatory Framework's provisions would not impact any current or future content regulation of traffic relating to cloud computing services accessed through the Internet from a location inside the KSA.

7.9.2 However, CSPs located in the KSA may also provide cloud services and distribute content to customers located outside the Kingdom. CITC is of the view that traffic originating or terminating in the datacentre of a CSP and that is only routed to or from international destinations will not need to be subject to KSA content regulation, provided such traffic is not accessible by users in the Kingdom without complying with such regulation.

Question 11: What are your views on the proposed treatment of content regulation described in this section and detailed in the Regulatory Framework (section 3.9)?

7.10 Other issues

7.10.1 The Type B class licenses available today include a **"telecommunications hotel license"** for services that are closely related to data hosting and certain cloud computing services. In CITC's view, the expected evolution of cloud services in the KSA and the proposed licensing regime for such services will phase out the market and regulatory justification for a separate license for telecommunications hotel services in the future.

7.10.2 Accordingly, it is proposed that these licenses should be eventually absorbed by cloud licenses (most probably CISLs). CITC is of the view that telecommunications hotel licenses will no longer be issued once cloud licenses become available. Further, the existing holders of telecommunications hotel licenses will be given a reasonable transition period to qualify for and migrate to cloud licenses.

7.10.3 In addition, the existing Type B **Internet Service Provider (ISP) licenses** allow the provision of web hosting among other services which now fall under the scope of the proposed cloud computing licenses. CITC is of the view that such an overlap should be avoided and that the provision of hosting services should be subject to a uniform set of rules.

7.10.4 Accordingly, it is proposed that ISP licenses should be adapted and licensees providing hosting services under an ISP license be given a reasonable transition period to qualify for and migrate their hosting services to cloud licenses.

Question 12: What are your views on the proposed approach regarding telecommunications hotel and ISP licenses?

8 Licensing of Cloud Computing

8.1 As described in Section 7.3, CITC envisages a licensing scheme with a number of categories of CSPs, based on factors such as the nature of the services offered, the handling of sensitive data, the size of commercial presence in the KSA or the location of the provider.

8.2 Apart from the Regulatory Framework's provisions on licensing, the following documents will be of relevance:

8.2.1 Application Procedure Guidelines for Cloud Computing Licenses

8.2.2 License provisions (including both CISLs and CSLs) and, as an alternative to CSLs proposed in this public consultation, a Cloud Service Declaration.

8.3 Application Procedure Guidelines

8.3.1 The Application Procedure Guidelines for Cloud Computing Licenses document is intended to provide clarity to CSPs on a number of practical issues related to the issuing of cloud computing licenses, including:

- Guidance on the need for, or benefits of, a license to operate their cloud services and the appropriate type of license (CISL or CSL) they should require, if any.
- Overview of the practical implications and benefits of a license.
- Description of the procedures and requirements for obtaining a license.

8.3.2 The Draft of the Application Procedure Guidelines for Cloud Computing Licenses is provided in Annex B.

Question 13: Are there any additional details or clarifications that you wish to see included in the definition of the applicable licenses and the CSPs that are required to operate under them?

Question 14: What are your views on the licensing procedures and requirements described in the draft of the Application Procedure Guidelines for Cloud Computing Licenses?

8.4 The 'Cloud Infrastructure and Services License' (CISL)

8.4.1 As indicated earlier, the 'Cloud Infrastructure and Services License' (CISL) is intended for CSPs that operate cloud computing infrastructure in the Kingdom, in order to offer cloud services directly or through third parties, or who control, store or process user content considered to be critical from an information security point of view (i.e., 'Level 3' user content).

8.4.2 By requiring these CSPs to obtain a 'Cloud Infrastructure and Services License', CITC is pursuing the following objectives:

- Identifying CSPs operating cloud computing infrastructure in the Kingdom, or controlling, processing and storing data considered to be critical in the KSA;
- Ensuring CITC's adequate knowledge of the location and basic technical features of critical cloud infrastructure in the Kingdom, such as datacentres;
- Increasing KSA cloud users' confidence in cloud services, particularly for sensitive data;
- Establishing formal points of contact between CITC and these CSPs, with adequate information, supervision and compliance mechanisms.

8.4.3 CITC expects that providers operating under a CISL will normally have a permanent presence or establishment in the KSA, in particular if they intend to run cloud computing infrastructure in the KSA. If the provider does not have a permanent establishment, it will be required to appoint a local representative.

8.4.4 The draft license document proposed for the CISL can be found in Annex C.

Question 15: What are your views on the objectives pursued by CITC with regard to the 'Cloud Infrastructure and Services License'?

Question 16: What are your views on the proposed provisions of the 'Cloud Infrastructure and Services License'?

8.5 The 'Cloud Services License' (CSL)

8.5.1 As indicated above, the 'Cloud Services License' is intended for cloud service providers or agents with a relevant activity in the Kingdom who do not need to operate cloud computing infrastructure in the KSA nor manage data considered to be critical from an information security point of view.

8.5.2 By requesting these service providers to obtain a CSL, CITC is pursuing the following objectives:

- Identifying CSPs providing cloud services in the KSA that exceed a minimum threshold of commercial presence.

- Establishing formal points of contact between CITC and these CSPs, with adequate information and some basic supervision requirements.

- Ensuring that these service providers have appropriate knowledge of the particular cloud regulations affecting their services in the KSA and are committed to complying with them.

8.5.3 Providers operating under the CSL may or may not have a permanent presence or offices in the KSA.

8.5.4 As an alternative to a CSL, and to reduce possible confusion with the CISL, CITC proposes a registration-based approach based on a declaration (further described in the Application Procedures Guidelines for Cloud Computing Licenses) filed with CITC by the CSP. This declaration would certify the CSP's agreement to comply with relevant regulations and certain basic obligations, which would be similar to those contained in the proposed draft text for the CSL. Taking into account the Respondents' comments,[2] CITC intends to opt for either the CSL approach or a registration approach.

8.5.5 The draft license document proposed for the 'Cloud Services License' can be found in Annex D. As mentioned in Annex E, in the event CITC decides to opt for a declaration procedure instead of a CSL, it is proposed that such a declaration should include, at a minimum, the information and commitments required under the draft application form for a CSL, and be subject to the same administrative fees.

2 In particular, their answers to Question 6.

Question 17: What are your views on CITC's objectives regarding the CSL?

Question 18: What are your views on the draft license document proposed for the CSL?

Question 19: What are your views on the proposal regarding the cloud service declaration, as an alternative to the CSL?

Question 20: What are your views on the overall regulatory scheme described in this document and in its annexes? Would you suggest any additional mechanism or measures to better promote and achieve the objectives described in section 5? Please provide supporting evidence for any recommendations or suggestions.

Annex A:
Draft Regulatory Framework on Cloud Computing

Contents

1. Introduction

1.1 Pursuant to Article 3 of the Telecommunications Act (the 'Act') the telecommunications sector must be regulated to, among other objectives, 'ensure creation of favourable atmosphere to promote and encourage fair competition in all fields of telecommunications.'

1.2 Council of Ministers Resolution no. 133 dated 21/5/1424H has expanded into the information technology field the powers of the Communications and Information Technology Commission ('CITC') and has entrusted it with the following, among other, tasks:

1.2.1 Implementing the policies, plans and programs approved for the development of information technology and setting out the appropriate procedures.

1.2.2 Proposing regulations and their amendments related to information technology, and pursuing approval of these regulations from the appropriate authorities.

1.2.3 Issuing the necessary licenses in accordance with the terms and acts related to them.

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

2. Definitions

2.1 The terms and expressions defined in the Act and the Telecommunications 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 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 involve the storage, transfer or processing of User Content in a Cloud System. The mere storage and processing of customer 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.

2.2.3 'Cloud 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 through Datacentres it owns and 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 Users.

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 he offers to Cloud Users.

2.2.4 'Cloud User' shall mean any Person making use of a CSP's Cloud Services. A Cloud User may also comprise multiple individuals or business units.

2.2.5 'Cloud Contract' shall mean an agreement for the provision of Cloud Services, concluded between a CSP and a Cloud User.

2.2.6 'Cloud System' shall mean an electronic information system comprising hardware, software and networking elements owned, controlled or operated by a CSP to supply Cloud Services to Cloud Users.

2.2.7 'Public Cloud' shall mean a Cloud System provisioned for open use by the general public.

2.2.8 'Private Cloud' shall mean a Cloud System provisioned for the exclusive use of an independent Cloud User.

2.2.9 'Hybrid Cloud' shall mean a combination of two or more Cloud Systems (both private and public) that are bound together by standardized or proprietary technology that enables data and application portability.

2.2.10 'Datacentre' shall mean a facility consisting of computing infrastructure and supporting components, housed in the same location, and used, in whole or in part, for the provision of Cloud Services.

2.2.11 'Content' shall mean any software, text, files, audio, images, graphics, illustrations, information, personal, business or other data, in any format.

2.2.12 'User Content' shall mean any Content provided or generated by a Cloud User 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 User.

2.2.13 'User Data' shall mean any data falling under at least one of the following categories, insofar as they are, or have been, part of the User Content or are, or have been, generated by the CSP with regard to one or more of its Cloud Users:

2.2.13.1 any data relating to an identified physical person who is a Cloud User or to such a Cloud User that can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors which allow that person to be identified;

2.2.13.2 any data relating to a Cloud User's business activities or financial affairs including, for example, its 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, unless the Cloud User has specifically approved the CSP's exclusion of some or all such business data from the above definition of User Data;

2.2.13.3 any data generated by, or for, the CSP concerning the Cloud User's activity log, billing, usage volume, statistics or other Cloud User-specific information associated with its use of the Cloud Services offered by the CSP.

2.2.14 'User Address' shall mean a Cloud User'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, User Address shall mean that address.

2.2.15 'Third Party Content' shall mean any Content, in electronic form, obtained or derived from any third party (other than the CSP) and made available to the Cloud User through, or in conjunction with, the Cloud User's use of the Cloud Services including, without limitation, data, information, software, documents, images, audio or video.

2.2.16 'Unlawful Content' shall mean User Content or Third Party Content that is unlawful under the laws of the Kingdom.

2.2.17 '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.

2.2.18 'Service Credits' shall mean discounts on current or future bills, time of Cloud Service added at the end of a billing cycle free of charge or similar compensation mechanisms offered by a CSP to a Cloud User if the CSP's actual performance fails to meet the standards set in the Cloud Contract or this Regulatory Framework.

3. Regulatory Framework

3.1 Scope

3.1.1 The provisions of this Regulatory Framework shall apply with regard to any Cloud Services provided to Cloud Users having a Residence or User Address in the Kingdom.

3.1.2 Without prejudice to Article 3.1.1, above, the following provisions of this Regulatory Framework shall also apply with regard to Cloud Services provided to any Cloud User as regards the processing or storage of their User Content and User Data, in whole or in part, permanently or occasionally, in Datacentres or other elements of a Cloud System that are located in the Kingdom:

3.1.2.1 Articles 3.3.12 (reporting on major information security breaches), below;

3.1.2.2 Articles 3.5.3 and 3.5.4 ('take-down' of Unlawful Content or User Content infringing intellectual property, upon CITC notice or by own initiative), and 3.5.5 (notification to CITC of violations of Anti-Cyber Crime Law), below; and

3.1.2.3 The exception referred to in Article 3.4.2.1, below.

3.1.3 Any obligations resulting from Article 3.1.1, above shall be binding on the CSP who owns, operates or offers access to the relevant Datacentres or other elements of a Cloud system located in the Kingdom, even if it is other than the CSP who has concluded the Cloud Contract with the Cloud User(s) in question.

3.1.4 Unless specified otherwise in this Regulatory Framework, these provisions shall be mandatory and not subject to any modification through contractual agreement.

3.2 Licensing [and registration] requirements

3.2.1 No Person may engage in any of the following activities or services except under and in accordance with a Cloud Infrastructure and Services License (hereafter 'CISL') issued by CITC to that Person:

3.2.1.1 the exercise of direct or effective control over Datacentres or other critical Cloud System infrastructure hosted in the Kingdom and used, in whole or in part, for the provision of Cloud Services;

3.2.1.2 the exercise of direct or effective control over the processing and/or storing of User Content classified as 'Level Three' User Content pursuant to Article 3.3 herein below.

3.2.2 No Person meeting the customer and/or turnover thresholds specified by the CITC pursuant to Article 3.2.3 below, may provide, under any capacity (such as a Cloud Provider, Cloud Broker, Cloud Aggregator, reseller, agent or any other category of CSP), Cloud Services to a Cloud User who has a Residence or User Address in the Kingdom, except [Alternative A: under and in accordance with a Cloud Services License (hereafter 'CSL') issued by CITC to that Person / Alternative B: following a registration as a CSP before CITC (hereafter 'CSP Registration')].

3.2.3 The licensing [and CSP Registration] requirements of Articles 3.2.1 and 3.2.2 shall be subject to the following exemptions:

3.2.3.1 A Person holding a CISL shall not need a [CSL] [CSP Registration].

3.2.3.2 A Person holding a Type (B) Class License for Internet Service Provider (ISP) Services shall not require [a CSL] [CSP Registration] to provide any of the services covered by the scope of the Type (B) Class License for Internet Service Provider (ISP) Services.

3.2.3.3 A Person holding a Type (B) Class License for the Service of Telecommunication Hotel shall not require a [CSL] [CSP Registration] to provide any of the services covered by the scope of that Type (B) Class License for the Service of Telecommunication Hotel.

3.2.4 The information to be provided for obtaining a CISL and a [CSL] [CSP Registration], any applicable thresholds, the relevant procedure to be followed for a CISL or a [CSL license] [CSP Registration] and any applicable fees shall be determined, and may be amended from time to time, by decision of CITC.

3.3 Information security

User Content Classification

3.3.1 User Content shall be subject to different levels of information security, depending on its sensitivity, origin and other criteria, as illustrated in the table below:

Classification of User Content by level of required information security	Categories of User Content for which each Level is normally intended
Level 1	Non-sensitive User Content of individuals, not subject to any sector-specific restrictions on the outsourcing of data
	Non-sensitive, public User Content of private sector companies or organizations, not subject to any sector-specific restrictions on the outsourcing of data
Level 2	Sensitive User Content of individuals, not subject to any sector-specific restrictions on the outsourcing of data
	Private (e.g. not aimed for publication) but non-sensitive User Content of private sector companies, not subject to any sector-specific restrictions on the outsourcing of data
	Public, non-sensitive User Content from public authorities already published, or aimed for publication, for general public access and deemed non-sensitive (e.g., public information (websites

Classification of User Content by level of required information security	Categories of User Content for which each Level is normally intended
Level 3	Sensitive User Content of private sector companies or organizations
	Any User Content from private sector regulated industries subject to a Level categorization by virtue of sector-specific rules or a decision by a regulatory authority
	Public sector User Content not in the public domain
	User Content qualifying for Level 1 or Level 2 treatment, for which the customer requests Level 3 treatment
Level 4	Highly sensitive or secret User Content belonging to concerned governmental agencies or institutions

3.3.2 This Regulatory Framework shall be applicable to User Content requiring a higher level of information security, as determined by other authorities.

3.3.3 The provisions of this Regulatory Framework shall be without prejudice to any applicable laws, regulations, guidelines, codes of conduct, internal instructions, corporate policies or any other legal, regulatory, administrative or corporate rules, concerning:

3.3.3.1 the Cloud Users' right, if any, to outsource, transmit, process or store in a Cloud System User Content or any data or information;

3.3.3.2 the Cloud Users' obligation to ensure that, if allowed, any such transmission, processing or storage should be subject to certain information security or data protection restrictions or safeguards, in addition to those specified to this Regulatory Framework.

Responsibility for User Content classification

3.3.4 Unless requested otherwise by the Cloud User concerned, CSPs operating under a CISL or a CSL must presume that the following levels of information security apply by category of Cloud User:

3.3.4.1 for natural persons with a Residence in the Kingdom: Level 1;

3.3.4.2 for private sector legal persons, such as companies, other corporate entities, associations or organisations incorporated or with a User Address in the Kingdom: Level 2;

3.3.4.3 for any government authorities or agencies: Level 3;

3.3.4.4 for all other categories: Level 1.

3.3.5 Cloud Users shall be free to inform their CSP, and responsible if they do so based on any obligations and duties that Cloud Users may have under any applicable rules outside this Regulatory Framework, of the level of information security applicable to, or desired for, part or the whole of their User Content if that level:

3.3.5.1 is not the one resulting from the presumptions of Article 3.3.4 above, or

3.3.5.2 is not Level 1 and the CSP does not operate under a CISL or a CSL.

Transfer and location of User Content

3.3.6 CSPs must ensure that no Level 3 User Content is transferred outside the Kingdom, for whatever purpose and in whatever format, whether permanently or temporarily (e.g. for caching, redundancy or similar purposes).

3.3.7 CSPs may not transfer, store or process Level 2 User Content to or in any Public Cloud or a Hybrid Cloud, unless they hold a CISL or a CSL.

3.3.8 CSPs may not transfer, store or process Level 3 User Content to or in any Public Cloud or a Hybrid Cloud, unless they hold a CISL.

3.3.9 Regardless of the level of information security (if any) required by the relevant Cloud User:

3.3.9.1 A CSP holding a CISL must disclose to CITC the location and main features of its Datacentres located in the Kingdom as well as of those located outside the Kingdom if they are implicated in the processing, storage, transit or transfer of User Data or User Content covered by this Regulatory Framework.

3.3.10 Without prejudice to their obligations under Article 3.3.6, CSPs must inform their Cloud Users in advance whether their User Content will be transferred, stored, or processed outside the Kingdom, permanently or temporarily.

Reporting of security breaches

3.3.11 CSPs must inform Cloud Users without undue delay of any security breach or information leakage that those CSPs become aware of, insofar as such breach or leakage affects, or is likely to affect, those Cloud Users' Cloud Content, User Data or any Cloud Services they receive from that CSP.

3.3.12 CSPs must inform CITC, without undue delay, of any security breaches or information leakage that those CSPs become aware, insofar as such breaches or leakages affect, or are likely to affect:

3.3.12.1 any Level 3 User Content,

3.3.12.2 the User Content or User Data of a significant number of Cloud Users or having an impact on a significant number of consumers in the Kingdom by virtue of their reliance on one or more Cloud Users' services, which are affected by the security breach or information leakage.

3.3.13 CSPs must inform their Cloud Users, upon their request, of the insurance coverage, if any, that those CSPs have for any civil liability to those Cloud Users, and of its essential features, insofar as these may be reasonably required for Cloud Users 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 Users or the CSPs they co-operate with, upon their request, a summary of these rules and policies.

3.4 Protection of User Data

3.4.1 The provisions of this Article 3.4 shall be binding upon CSPs who:

3.4.1.1 conclude a Cloud Contract with a Cloud User, as well as

3.4.1.2 those who, although not a party to such a Contract with the Cloud User concerned, alone or jointly with others determine the purposes and means of the processing of the relevant Cloud User's User Data.

3.4.2 CSPs may not provide, or allow another party to provide, to any third party (including, but not limited to, any individuals, legal entities, domestic or foreign government or public authorities) User Content or User Data belonging to a Cloud User, or process or use them for purposes other than those allowed under the Cloud Computing Agreement, unless:

3.4.2.1 they are required to do so under the laws of the Kingdom; or

3.4.2.2 the User Data is Level 1 or Level 2 Data, and the relevant Cloud User provides its express prior consent, whether in the form of an 'opt-in' or the form of an 'opt-out', which the Cloud User shall remain free to withdraw at any time in the future.

3.4.3 CSPs shall grant Cloud Users the right and the technical possibility to access, verify or delete their User Data.

3.4.4 The provisions of this Article 3.4 shall be without prejudice to any applicable legal, regulatory or contractual provisions 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 User Data or User Content covered by this Regulatory Framework.

3.5 Unlawful content and Intellectual Property

3.5.1 Subject to the provisions of this Article 3.5, a CSP shall not incur any administrative or criminal liability based only on the fact that Unlawful Content or User Content that infringes a third party's intellectual property rights has been uploaded, processed or stored on the CSP's Cloud System.

3.5.2 Nothing in this Regulatory Framework shall be interpreted as a legal obligation for CSPs to actively and constantly monitor their Cloud System for Unlawful Content or User Content that infringes any third party's intellectual property rights.

3.5.3 CSPs must remove or render inaccessible in the Kingdom and/or (if this is required under the Kingdom's international obligations) any other jurisdiction, any User Content on their Cloud System that includes Unlawful Content or infringes a third party's intellectual property rights, if the CSPs are ordered to do so by CITC and/or any other authorized entity in the Kingdom.

3.5.4 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 Unlawful Content or User Content that allegedly infringes a third party's intellectual property rights, provided this is in accordance with the provisions of the Cloud Contract.

3.5.5 CSPs must notify CITC and/or any other authorized entity, without undue delay, if they become aware of the presence of any User Content or other information on their Cloud System that may constitute a violation of Anti-Cyber Crime Law.

3.5.6 CSPs must refer any third parties complaining against Unlawful Content on their Cloud System to the competent authorities in the Kingdom.

3.5.7 CSPs may inform a Cloud User that Unlawful Content found in his Cloud Content has been taken down unless CITC and/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 CSP's to inform the Cloud User about the taking down of his Cloud Content threatens to create any liability of the CSP.

3.5.8 The provisions of this Article 3.5 shall be without prejudice to the CSPs' obligation to co-operate with the Kingdom's authorities, pursuant to any applicable laws or the provisions of their license, in law enforcement matters associated with unlawful content.

3.5.9 CSPs must grant their Cloud Users all necessary and lawful licenses for the use of any software or other legally protected intellectual works in the Cloud Services provided under their Cloud Contract, commensurate to the duration and scope of the Cloud Contract.

3.5.10 CSPs must indemnify and hold harmless their Cloud Users against any claims by a third party for any breach of intellectual property rights, under the laws of any jurisdiction, insofar as such breach is caused through the Cloud System's internal operations or the software licensed by the CSP to the Cloud User, but not if the breach has been caused through the Cloud User's infringement of the terms of the licenses mentioned in Article 3.5.9, above or his other obligations under the Could Contract.

3.6 Information on Cloud Contracts and minimum mandatory articles and provisions

3.6.1 Prior to the conclusion of a Cloud Contract with a Cloud User, and without prejudice to any other additional information that CSPs may need to communicate to Cloud Users if so required under their license or other applicable laws, CSPs must provide clear and transparent information to that Cloud User on the object of the service, the conditions of use, Cloud Service levels, and applicable payment terms.

3.6.2 Upon request of by an existing or potential Cloud User, CSPs must present to that Cloud User proof of the CSP's authorization, through a license and/or a contract with another CSP, to use, directly or indirectly, the Datacentres and other infrastructure required for the provision of Cloud Services by that CSP to the Cloud User concerned.

3.6.3 Without prejudice to any other obligations 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, business address and full contact details;

3.6.3.2 description, and allowed use of the services to be provided;

3.6.3.3 contract duration, applicable charges, payment terms and termination;

3.6.3.4 rules on handling of User Content, including its processing, destruction and restoration to its original version upon Cloud Contract termination

3.6.3.5 a Service Level Agreement (SLA);

3.6.3.6 a procedure for the resolution of customer 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 customer care service for the resolution of any customer complaints that shall be separate from, and without prejudice to, any other legal remedies and dispute resolution procedures available under applicable laws, also including this Regulatory Framework.

3.6.5 Cloud Users and CSPs shall have a right to refer their disputes, jointly or separately, to any dispute resolution procedures available before CITC pursuant to CITC Statutes.

3.6.6 Upon termination of the Cloud Contract with a Cloud User, and if the Cloud User so requests, the CSP must:

3.6.6.1 provide to the Cloud User a copy of the Cloud User's Cloud Content stored on the CSP's Cloud System at the time of the Cloud Contract's termination, or (if the Cloud User agrees to such an alternative) allow and offer the Cloud User the means to download such Cloud Content provided that, in both of these cases, the CSP shall ensure that the Cloud Content is provided to the Cloud User in a commonly used format;

3.6.6.2 as an alternative to the options of Article 3.6.6.1,above, transfer the Cloud User's Cloud Content, in a suitable format, directly to another CSP of the Cloud User's choice, where this is technically feasible.

3.7 Consumer protection and unfair contract terms

3.7.1 CSP shall be liable to its Cloud Users for any acts or omissions by the CSP, its agents, subcontractors, resellers or employees (acting within the framework of their agency, employment, subcontracting or reseller relationship with the CSP), incurring liability to such Cloud Users 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 Cloud Users for (i) any loss of, or damage to, User Content or User Data; (ii) 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 User concerned or with the provisions of any mandatory legal provisions; or (iii) information security breaches or information leakage, provided, in all of these cases, that the resulting loss or damage may be reasonably attributed, in whole or in part, to intentional or negligent acts or omissions of the CSP concerned.

3.7.3 A 'best efforts' clause by a CSP in a Cloud Contract may not exclude its liability to Cloud Users for acts or omissions committed intentionally or through negligence.

3.7.4 CSPs shall bear the burden of proof that any loss or damage referred to in Articles 3.7.1 and 3.7.2 above may not be reasonably attributed, in whole or in part, to intentional or negligent act or omissions for which they are solely or jointly responsible.

3.7.5 Notwithstanding the above, CSPs may:

3.7.5.1 Exclude or limit their liability for any indirect damages or any loss of revenue or profits, provided that this is caused non-intentionally to a Cloud User;

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 User under his Cloud Contract with the CSP and/or compensate the Cloud User through Service Credits;

3.7.5.3 in the case of liability for information security breaches or information leakage, limit their liability if the Cloud User (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 information security risks.

3.8 Quality Standards

3.8.1 CSPs subject to a CISL or a [CSL] [CSP Registration] must:

3.8.1.1 Inform their Cloud Users, upon request, of the actual levels of achievement of any SLA requirements 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 Users, upon request, of any certification systems or standards that these CSPs meet with regard to their Cloud Services to the relevant Cloud User;

3.8.1.3 comply with any certification schemes and/or standards (including encryption standards) that may be defined as mandatory by CITC decision with regard to Cloud Computing;

3.8.1.4 comply with any rules or guidelines adopted by CITC with regard to business continuity, disaster recovery and risk management.

3.8.2 Encryption by Cloud Users of their User Data or Content shall not affect the CSPs' obligations under this Regulatory Framework.

3.8.3 CITC may issue, from time to time, decisions on mandatory or voluntary certification schemes and standards for Cloud Computing, which may vary depending on the required level of information security, the type of CSP or Cloud User concerned, or by other criteria.

3.9 Content Regulation

3.9.1 User Data or Content in a Cloud System to which this Regulatory Framework applies may be excluded from content regulation by a CITC decision if such User Data or Content

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 an independent Cloud User.

3.9.2 The provisions of Article 3.9.1, above shall be without prejudice to any other rules or decisions on content regulation that may be adopted by any other authorized entity in the Kingdom.

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 CITC Statutes, without prejudice to any penalties that may be imposed under any other applicable laws in the Kingdom, including, in particular, the Anti-Cyber Crime Law (issued under the Council of Ministers Decision No. 79, dated 7/3/1428 H, 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 7/3/1428 H 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 Without prejudice to the generality of the above, CITC may take any action allowed under CITC Statutes to prevent a Licensee in breach of this Regulatory Framework from providing Cloud Services in the Kingdom, either fully or (if only certain of this Licensee's Cloud Services are found to be in breach) in part.

3.10.3 CITC may issue guidelines, model Cloud Computing contracts or clauses, guides, recommendations or other texts aimed at:

3.10.3.1 clarifying any aspects of the present Regulatory Framework;

3.10.3.2 providing guidance to CSPs, Cloud Users and the public in general on any aspects of Cloud Computing;

3.10.3.3 complementing this Regulatory Framework through mandatory or voluntary detailed implementation provisions.

Annex B:
Application Procedure Guidelines for Cloud Computing Licenses

Table of Contents

1 Introduction

This document provides practical guidance on the types and content of cloud computing licenses available in the Kingdom and their implications, the eligible cloud service providers (CSPs) and the procedures required to obtain such licenses.

Under the Regulatory Framework on Cloud Computing (the 'Regulatory Framework') CITC may issue two types of licenses for the provision of cloud computing services: A Cloud Infrastructure and Services License ('CISL') and a Cloud Services License ('CSL'). The Regulatory Framework also allows CITC to exempt CSPs from any such licensing requirements, if they do not have a significant commercial presence on the Kingdom in terms of a minimum number of Cloud Users, turnover or other objective criteria.

In exercise of these powers, CITC has issued a CISL (see Annex 'C') and a CSL (see Annex 'D'), each meant to apply to different types of CSPs.

Cloud computing involves different types of services and providers, a rapidly evolving market, and jurisdictional questions that are sometimes difficult to resolve because of the Cloud's international nature. As concluded in the recent CITC report on 'Datacenter, Managed and Cloud Services in Saudi Arabia': "the lines between provider categories are not definitive, due to a significant amount of crossover. It is likely that this blurring of borders will continue, resulting in a highly converged ICT ecosystem where traditional technology provider categories will no longer be relevant."

Under these circumstances, the exact distinction between different types of CSPs requiring different types of cloud computing licenses may not always be clear cut and can therefore benefit from regulatory guidance and examples.

Accordingly, the first part of these Guidelines provides details on the categories of CSPs that (i) require a CISL, (ii) require a CSL and (iii) do not require any cloud computing license. This section will be followed by:

- A short review of the implications of each of the two types of available licenses.
- A clarification of the licensing requirements, if any, applying to international CSPs offering their services in the KSA.
- The more practical aspects of the application procedure, documentation and application fees associated with each of the CISL and the CSL.

The meanings assigned to the terms used in these Guidelines were taken from the relevant definitions in the Regulatory Framework, the Telecommunications Act or the Telecommunications Bylaw.

IMPORTANT NOTICE: As indicated in the public consultation, CITC is seeking out views from stakeholders regarding the option to require a mere registration rather than a CSL for CSPs belonging to the second of the three categories of CSPs defined for licensing purposes. We note, however, that these Application Procedure Guidelines have been drafted on the assumption that a cloud services license (CSL) would be required for such CSPs. Sections describing the applicable procedures to obtain a CSL, as well as the implications of obtaining such a license, would therefore not be directly applicable if CITC opts for a registration procedure for these CSPs. However, in that case, these sections will apply by analogy regarding the discussion on the CSPs requiring such a registration as opposed to a CISL.

2 Licensing Requirements for Cloud Service Providers in the KSA

2.1 Which cloud services may require a Cloud Computing License in Saudi Arabia?

Cloud services are subject to the Regulatory Framework, and therefore also its provisions on licensing,[1] insofar as they are provided to cloud users having a residence or a user address in the Kingdom.[2]

The Regulatory Framework defines cloud services as "information and communications technology (ICT) services provided through Cloud Computing, which involve the storage, transfer or processing of User Content in a Cloud System, unless such services are limited to the storage of certain data relating to one or more persons (such as their names, addresses or transaction-related data)".[3]

This definition of cloud services implies that a first key criterion for determining whether a CSP may require a cloud computing license is whether the services it provides involve the handling (i.e., the storage or processing) of user content, a term defined in the Regulatory Framework as including "any software, text, files, audio, images, graphics, illustrations, information, personal, business or other data, in any format," that are "provided or generated by a Cloud User" and which are "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 User".[4]

Such services are subject to regulation regardless of whether the storage and/or processing of user content is provided in 'raw' form, for instance under an IaaS model, or as part of a broader bundle of services, which may include the licensing of software or other technical capabilities, such as processing or data transmission capabilities. The assessment of whether such services are subject to the Regulatory Framework is also independent of whether the user content is intended to be made public (i.e., accessible by anyone), to be shared among a restricted set of users or to remain private.

For instance, a CSP may offer:

- A service to manage, edit, create or manipulate certain categories of user content under a Software as a Service (SaaS) model which, technically, requires the storage and processing of that user content in the cloud system of the CSP.

- A service that allows cloud users to share their user content with others by uploading pictures, videos, documents or any other form of proprietary content to a cloud-enabled platform run by the CSP.

In both of these examples, such CSPs would be subject to the Regulatory Framework and its associated rules when providing their services in the KSA. Accordingly, they may need a license to provide their services in the KSA if they meet the conditions stated

1 Regulatory Framework, Article 3.2.
2 Regulatory Framework, Article 3.1.1.
3 Regulatory Framework, Article 2, Definitions.
4 Please refer to the Definitions of 'Content' and 'User Content' in Article 2.2.14 and 2.2.15 of the Regulatory Framework.

below in sections 2.2 and 2.3 of these Guidelines.

If the services that a CSP provides do not involve the handling of user content, then such CSP would not require a cloud computing license.

This may be the case, for example, with service providers that:

- Distribute their own content (or content licensed to them by third parties) making use of the cloud.

- Distribute or store content partially generated by users, when such content does not actually belong to them, such as in the case of reviews or opinions generated by users in a cloud-powered platform.

- Operate services making use of the cloud that do not involve the storage or processing of user content, but do require the handling of User Data, such as names, address, invoicing and payment details or transaction-related records. An example would be service providers operating e-commerce activities, or simply using cloud-enabled communications to facilitate their interface with users – even if such cloud-enabled communication is an essential part of the value proposition.

The statement that certain services provided over the cloud may not require a cloud computing license should not be misunderstood as meaning that such services are necessarily free of any regulation in the KSA. Based on the nature of each specific service that they provide, service providers may be subject to regulations other than those pertaining to cloud computing, and to rules and regulations other than those established by CITC.

For example, services provided over the cloud that involve the provision of telephony or similar communication services may require separate licenses from CITC. Other services may require approvals and/or administrative licenses or permits from the relevant sector-specific regulatory bodies in the KSA or other government agencies. Nothing in these Guidelines should be understood as relieving service providers from their responsibility to ensure that their services are compliant with any sector-specific or general regulations and laws in the Kingdom applicable to their particular business models and services.

2.2 Which Cloud Service Providers require a Cloud Infrastructure and Services License (CISL)?

CISLs are generally required for all CSPs wishing to provide any type of cloud computing services through datacentres or other critical infrastructure, equipment and other elements of 'cloud infrastructure' which they own, construct and/or control in the territory of the Kingdom. Under a CISL, such cloud infrastructure may be used, in whole or in part, for the provision of

cloud computing services to cloud users with a residence or user address in the Kingdom and/or to such users located anywhere else in the world. The licensing requirements remain the same in all cases.

Similarly, the licensing requirements will not be affected by the type of cloud computing service provided by the CSP (SaaS, PaaS, IaaS or other) or the deployment model offered (public, private or hybrid).

A CISL license will also be required for CSPs that own or operate such cloud infrastructure and equipment in the Kingdom but provide cloud services to end users only indirectly, through other parties such as cloud brokers, cloud aggregators, resellers, etc.

Finally, a CSP will need to obtain a CISL even if it does not meet any of the above conditions, but wishes to extend its cloud services in the Kingdom to certain categories of user content considered sensitive and hence classified as 'Level 3' user content from an information security viewpoint, pursuant to the Regulatory Framework's relevant provisions.

The Regulatory Framework includes a (rebuttable) presumption that any user content belonging to the Government, State or public services or agencies will fall under such a 'Level 3' level of information security if not higher (in which case it will fall outside the scope of the Regulatory Framework and is likely subject to stricter provisions). In addition, Level 3 user content can include sensitive user content of private sector companies or organisations, and user content from private sector but regulated industries, such as hospitals or financial institutions, that may be subject to sector-specific rules.

Note that, in such cases, it will be the cloud user's responsibility to decide whether to use cloud services and to indicate to the CSP the level of information security. Similarly, Government, State or public services or agencies may decide, based on their own responsibility and internal rules, that certain types of user content they wish to outsource to a cloud are not sensitive and can therefore be also treated as Level 2 or Level 1 user content.

The CISL allows the provision of licensed services in the entire territory of the Kingdom.

2.3 Which Cloud Service Providers require a Cloud Services License (CSL)?

Essentially, CSLs will be required for CSPs that offer cloud services to users with a residence or a user address in the Kingdom, provided these CSPs (i) do not own, operate or control any cloud infrastructure in the Kingdom and (ii) do not exercise effective control over the processing and storage of the 'Lever 3' user content discussed above.

CITC expects that CSLs will be required for:

- Various categories of CSPs that provide their services to users in the Kingdom but do not have or operate their own cloud infrastructure, such as cloud brokers or cloud resellers.

- CSPs operating outside the Kingdom, with or without their own cloud infrastructure, but only in relation to the cloud services they provide to cloud users with a residence or cloud address in the Kingdom.

- International CSPs that wish to provide cloud services in the Kingdom by leasing capacity on the cloud system of an established service provider in the Kingdom equipped with the necessary CISL. In such cases, the international CSPs can exercise effective control over the processing and storage of Level 1 or Lever 2 user content, using another CSP's cloud infrastructure in the Kingdom.

As is the case with the CISL, the CSL allows the provision of licensed services in the entire territory of the Kingdom.

2.4 Which Cloud Service Providers do not require a Cloud Computing license?

According to CITC, CSPs that would normally need a CSL to operate under the previous criteria, should not be required to obtain this or any license if their commercial presence in the Kingdom with regard to the provision of cloud services does not exceed a certain threshold. That threshold consists of two alternative criteria: the number of cloud users with a residence or cloud address in the Kingdom, and the CSP's revenues attributed to such cloud users.

The combined application of these two criteria is necessary to address two basic types of cloud services and cloud users. Cloud services that are addressed to the general public, typically individuals, can rapidly obtain a significant number of users but a relatively low level of revenues per user. On the other hand, B2B cloud services can generate significant revenues per cloud user, if that cloud user is a corporate entity or organisation with a potentially high number of individual employees or other staff making use of the cloud service.

Accordingly, CITC will not require a CSL license for CSPs that otherwise meet the criteria for such a license but have less than 10,000 cloud users with a residence or cloud address in the Kingdom and less than 1 million SAR of revenue from the KSA. These thresholds may be revised by the CITC in the future.

As stated in section 2.1, service providers that exclusively offer services that do not fall within the Regulatory Framework's definition of cloud services will also not require a cloud license.

2.5 What are the implications (benefits and obligations) of operating under a cloud license in the Kingdom?

2.5.1 Implications for both types of licenses

The basic implication of operating under either one of the two cloud licenses is that they give the CSP a clear regulatory status, and clearly defined rights and obligations in the Kingdom. CITC believes that both public authorities and, at least, larger corporate users will prefer to engage such licensed CSPs, as their licensed status provides certain guarantees of security and reliability, and a clearer set of rights and obligations. Indeed, cloud users wishing to outsource sensitive (Level 3) content to the cloud will have to deal with CSPs holding a CISL license.

Thus CSP licenses are likely to generate certain advantages for their holders, both for legal reasons (e.g., requirement of a CSL license for Level 3 user content) and commercial reasons. Consequently, CSPs wishing to compete for the provision of B2B or other, higher

end, cloud computing services in the Kingdom but do not yet have the necessary local cloud infrastructure, number of cloud users in the Kingdom or associated revenues, may still wish to obtain a license in order to compete more effectively and upgrade their profile in the local market.

Accordingly, CSPs are free to apply for a license even if they do not need one as a legal obligation, i.e.:

- CSPs that do not require any license (see Section 2.4, above) may apply for a CSL or a CISL.

- CSPs that require only a CSL may apply for a CISL.

In both of these cases, the applicants will receive the license they apply for if they provide the information and commitments requested in the appropriate application form (see Section 3, below). Once they obtain such a license, they will have all the rights and obligations associated with the license in question, as specified in text of the license itself, as well as in the Regulatory Framework.

Obtaining a license may raise questions about the transition of existing cloud users. For example, under the new cloud licensing framework, CSPs offering their services to cloud users in the Kingdom today without any license may have a legal obligation or (in its absence) a commercial interest in obtaining a CSL or a CISL. As another example, in the future, holders of a CSL may wish or be obliged to obtain a CISL.

Under both of these examples, once they obtain such a license, these CSPs may not distinguish between two different classes of cloud users (pre-license and post-license). Accordingly, they must provide a commitment in their license application to extend the terms of the license to any and all of their existing clients with a residence or user address in the Kingdom, within a transitional period of no more than one month from the effective date of the license.

2.5.2 Implications for CISL holders

Although CISL and CSL holders are, in principle, subject to broadly similar obligations under the Regulatory Framework, in practice the holders of CISLs will have a more extensive set of obligations associated with their cloud systems in the KSA, in regards to matters such as information security, data protection, unlawful content, their cloud contracts' minimum content and quality of service (especially in the future, if certain certification standards are adopted). The application for a CISL will require the payment of a one-time application fee of 50,000 SAR.

On the other hand, CISL holders also enjoy certain rights that are not available to CSPs under a CSL. In addition to their right to handle Level 3 user content, they also have the right to build and/or operate datacentres in the Kingdom for the provision of cloud services to the public, as well as to connect their infrastructure and network elements with any licensed ISP or facilities-based service provider in the Kingdom. In this second case, they may also obtain international connectivity access directly from international providers.

2.5.3 Implications for CSL holders

The CSL provides an easy way for CSPs to obtain a regulated status in the KSA market – thus largely avoiding legal uncertainty– without a need to invest in their own local cloud infrastructure and possibly even without any local corporate or physical presence, as long as the applicant can provide an address in the Kingdom.

On the other hand, CSL holders do not enjoy the right to build or operate datacentres in the Kingdom, or the associated direct interconnection rights of CISL. This is consistent with the idea that they do not own or control any cloud infrastructure in the Kingdom.

2.6 International CSPs and licensing

In principle, the Regulatory Framework applies to any cloud services that are provided to cloud users with a residence or user address in the Kingdom, regardless of the location of the CSP. Thus, in principle, any CSPs serving cloud users in the Kingdom will require a license by CITC, unless they can benefit from the exception stated above, based on their limited commercial presence in the Kingdom. Their need for such a (CSL) license will not be conditional on a corporate establishment or subsidiary in the Kingdom, but will also not require establishing such a presence, other than an address for service.

CSPs owning or using cloud systems located in the Kingdom are also free to provide their cloud services to cloud users with a residence or user address outside the Kingdom, in other jurisdictions. In principle, the relationships between the CSP and those cloud users will be governed by the rules of those other jurisdictions. Only a few provisions of the Regulatory Framework, set forth in its Article 3.1.2 apply also with regard to this type of 'outbound' CSP activity, and these do not include those concerning licensing.

Thus the provision of cloud services to cloud users who do not have a residence or a user address in the KSA

- Is not a licensable activity, as such, under the Regulatory Framework, regardless of whether these services are provided, in whole or in part, from a cloud system hosted in the Kingdom; but

- is not an entirely unregulated activity either, as the CSPs providing such services will need to comply with the minimal set of provisions mentioned in Article 3.1.2 of the Regulatory Framework.

2.7 Licensing and subcontracting

As should be clear from the preceding explanations, a requirement for a cloud computing license by CITC is not necessarily conditional on the physical presence of the eligible service provider's cloud system in the Kingdom. Such a service provider may use its own cloud system hosted outside the Kingdom, but may also rely solely on capacity leased, subcontracted or otherwise provided by another CSP in the Kingdom or elsewhere. A license may be required in all these cases.

The critical condition triggering such a licensing requirement is the provision of cloud services, based on cloud contracts concluded between the eligible service provider and cloud users in the Kingdom, and a commercial presence in the Kingdom above the minimum KSA cloud user number or KSA revenues mentioned in section 2.4, above. If these conditions are met, the mere fact that the CSP is acting as the contractor of another service provider (which owns or controls the relevant cloud system, directly or through a chain of similar leasing, licensing or subcontracting arrangements) is not sufficient to exempt that CSP from the need to obtain a cloud computing license.

On the other hand, a mere CSL may be sufficient in some of these cases: as mentioned above, a CSP may choose to store user content or user data in the KSA, in a cloud system operated and controlled by another CSP (which would normally need to have obtained a CISL for this purpose). Mere use of such infrastructure by the first CSP will not necessitate a CISL.

3 Application Procedure and Documentation

3.1 Procedure for obtaining a CISL or a CSL

The grant of a CISL or a CSL requires the submission of an application by the interested party to CITC, through the application form adopted for this purpose, attached hereto as Appendix 'A' (for a CISL) and Appendix 'B' (for a CSL), both of which can be downloaded from CITC website (www.citc.gov.sa).

The application form for a CISL must be completed in Arabic; the one for the CSL must be completed in Arabic or English.

Any certificates, separate declarations or similar documents attached to the CISL must be also in Arabic or accompanied by an official Arabic translation. No such translation will be necessary for more general information provided by the Applicant, such as annual reports or brochures.

For both licenses, the application form and its attached documentation must be submitted in paper form to CITC's address.

CITC has the right to publish a list of the granted CISLs and CSLs and the names, contact details and services provided by each license holder.

3.2 Required Documentation

The CISL Application Form must be accompanied by:

- Proof of payment of the license application fee through SADAD payment system after getting the invoice number by contacting the Revenue Department, CITC, at any of the following telephone number (0114618151) fax (0114618045).

- Bank Guarantee for an amount of 100,000 SAR as per the form set by CITC and available on CITC's website, from a local bank in Saudi Arabia, approved by SAMA, in Saudi Riyals. The bank guarantee validity term shall be equivalent to that of the License.

- True certified copy of the authorized signatory(ies)'s official ID(s);

- In the case of legal persons, proof of that person's existence in law (such as a certified extract or certificate from the register of companies, firms or associations or any other official document).

- In the case of legal persons, proof of the signatory(ies)'s authority to act on behalf of the applicant (such as a power of attorney or a company resolution).

The dates of the above documents or their relevant certifications may not be older than 6 months from the application date.

The CSL Application Form must be accompanied by:

- True certified copy of the authorized signatory(ies)'s official ID(s).

- In the case of legal persons, proof of that person's existence in law (such as a certified extract or certificate from the register of companies, firms or associations or any other official document).

- In the case of legal persons, proof of the signatory(ies)'s authority to act on behalf of the applicant (such as a power of attorney or a company resolution).

List of Appendixes

Appendix 'A' CISL Application Form

Appendix 'B' CSL Application Form

Appendix 'A' CISL Application Form

1. Information on the Applicant

Name of Company or Corporation (in Arabic): .....

CR No; .....

Name of Company or Corporation (in English): .....

Address of registered seat or main place of business:

.....

.....

.....

.....

.....

.....

Tel: .....

Fax: .....

Website: .....

Name of Signatory:.....

Position:.....

Professional address:.....

.....

.....

Tel (fixed): .....

Tel (mobile): .....

Fax: .....

email: .....

Name of an authorised representative in the KSA (if other than the Signatory and the Applicant's address is not in the KSA):

.....

Position:.....

Professional address:.....

.....

.....

Tel (fixed): .....

Tel (mobile): .....

Fax: .....

email: .....

Please provide, as an attachment, proof of the authorization granted by the Applicant to the above person to act as the Applicant's representative.

Please provide brief information on the Applicant's ownership structure, mentioning any affiliates or joint ventures it has in the KSA and the ultimate owners of the company applying for a license.

2. Information on the Applicant's Cloud Activities

Indicate the type of cloud service(s) you plan to provide or are providing already to cloud users with a residence or user address in the KSA (you may check more than one box):	
☐	Cloud services directly to the public in the KSA
☐	Hosting ICT devices and equipment, and providing interconnection services between these devices and CITC-licensed infrastructure-based ICT service providers
☐	Exercising direct or effective control over the processing and storing of user content and user data[5] in the Kingdom
☐	Constructing and operating datacentres and associated infrastructure for the provision of Cloud Services, directly or through other, duly licensed or otherwise entitled, third parties
☐	Other (please provide details below)

5 These and any other terms used in this Application Form have the meaning ascribed to them in the Regulatory Framework on Cloud Computing.

3. Information on the Applicant's Cloud System

Please provide, on one or more separate pages attached to this form, a succinct description of the cloud system(s) you use or intend to use for the provision of cloud services to cloud users in the KSA including, in particular:

- Any datacentres located in the territory of the KSA, with their full address, contact details (tel/fax/email) and website
- The relationship that best describes your access to this datacentre's capacity and infrastructure (e.g., owner, operator, co-owner, lessor or lessee of capacity, reseller, etc.)

  Please provide, on one or more separate pages attached to this form, a succinct description of any networking or other key equipment associated with the above datacentres and the relationship that best describes your access to, and use of, such key equipment.

  You may also attach any available technical brochures, website printouts or other technical and commercial information related to the cloud system(s) you use or intend to use for the purposes of this license.

4. Information on the Applicant's Other Activities

Please provide a brief (100-200 words) description of the operations, in the KSA and elsewhere, of your company and the group it belongs to (if any). You may also provide a link to the most recent annual report (if available), financial reports or other statements covering the Applicant's operations.

Please provide a list of any licenses held to date in the KSA, granted by CITC to (i) the Applicant, (ii) any affiliate of the Applicant or (iii) any joint venture in which the Applicant or an affiliate of the Applicant participates.

5. Commitments by the Applicant

I, the undersigned, acting for and on behalf of ..... ('the Applicant') acknowledge, certify and agree that:

- the information provided in this Application Form and its attachments is true and correct;
- the Applicant shall comply with the terms and conditions of the Cloud Infrastructure and Services License applied for, and those of the Regulatory Framework (also including Article 3.1.2), the Guidelines, and any CITC statutes, as well as with any future amendments to the above;
- the Applicant shall extend, no later than one month from the effective date of this License, its terms and conditions to its existing cloud users (if any) with a residence or user address in the Kingdom;
- the Applicant shall inform CITC immediately of any changes to the information provided under heading (1) above ('Information on the Applicant') and any material changes to the information provided under headings (2) ('Information on the Applicant's Cloud Activities') or (3) ('Information on the Applicant's Cloud System'), above;
- the Applicant accepts that CITC may publish any of the information provided by the Applicant in this Application Form except any such information reasonably qualifying as a confidential business secret, provided that the Applicant has identified this information in a separate attachment to this Application Form and has provided an explanation, to CITC's reasonable satisfaction, of the reasons why it should not be disclosed to the public.

_____ _____

Name, Title and Signature Place and Date

Appendix 'B' CSL Application Form

1. Information on the Applicant

Name of Company or Corporation (in Arabic), if applicable: .....

CR No: .....

Name of Company or Corporation (in English): .....

Address of registered seat or main place of business:

.....

.....

.....

Tel: .....

Fax: .....

Website: .....

Name of Signatory:.....

Position:.....

Professional address:.....

.....

.....

Tel (fixed): .....

Tel (mobile): .....

Fax: .....

email: .....

Name of a Contact Person (if other than the Signatory)

.....

Position:.....

Professional address:.....

.....

.....

Tel (fixed): .....

Tel (mobile): .....

Fax: .....

email: .....

Address for service in the KSA:

.....

.....

.....

.....

Tel: .....

Fax: .....

2. Information on the Applicant's Activities

Please provide a brief description of the type of cloud service(s) you plan to provide or are providing already to cloud users with a residence or user address in the KSA, and the technical means (cloud system, networking elements, etc.) relied upon for the provision of these services.
Please provide a list of any licenses held to date in the KSA, granted by CITC to (i) the Applicant, (ii) any affiliate of the Applicant or (iii) any joint venture in which the Applicant or an affiliate of the Applicant participates.

5. Commitments by the Applicant

I, the undersigned, acting for and on behalf of ..... ('the Applicant') acknowledge, certify and agree that:

- the information provided in this Application Form and its attachments is true and correct;
- the Applicant shall comply with the terms and conditions of the Cloud Services License applied for, and those of the Regulatory Framework (also including Article 3.1.2), the Guidelines, and any applicable CITC statutes, as well as any future amendments to the above;
- the Applicant shall extend, no later than one month from the effective date of this License, its terms and conditions to its existing cloud users (if any) with a residence or user address in the Kingdom;
- the Applicant shall inform CITC immediately of any changes to the information provided under heading (1) above ('Information on the Applicant');
- the Applicant accepts that CITC may publish any of the information provided by the Applicant in this Application Form except any such information reasonably qualifying as a confidential business secret, provided that the Applicant has identified this information in a separate attachment to this Application Form and has provided an explanation, to CITC's reasonable satisfaction, of the reasons why it should not be disclosed to the public.

_____ _____

Name, Title and Signature Place and Date

Annex C:
Draft Cloud Infrastructure and Services License (CISL)

License Number:_____

Cloud Infrastructure and Services License (CISL)

[Draft]

Issued to:

Company/Establishment:_____

Date of issue of this license __ /__ /____ (H) equivalent to __ /__ /____ (G)

Expiry date of this license __ /__ /____ (H) equivalent to __ /__ /____ (G)

Commercial Registration Number: _____

Date of issue of CR __ /__ /____ (H) Expiry date of CR: __ /__ /____ (H)

Issuing Location of CR: _____

Phone: _____ Fax: _____ Box: _____

Postcode: _____

Based on the Telecommunications Act issued by Royal Decree (M/12) dated 12/3/1422 and its Bylaws, and in accordance with the Communications and Information Technology Commission ('CITC') Ordinance issued under the Council of Ministers Decision No. (74) dated 5/3/1422, CITC has issued this License to the company/establishment above in accordance with the following conditions and annexes which together comprise integral parts of this License:

- License Terms & Conditions
- Appendix (1) Fee Schedule

Official Seal

Table of Contents

Cloud Infrastructure and Services License (CISL) Terms and Conditions

Article 1: Definitions

1. The words and expressions defined in the Telecommunications Act, its Bylaws, the Ordinance of the Communications and Information Technology Commission ('CITC') and the Regulatory Framework on Cloud Computing shall have the same meanings in this License.

2. The following words and expressions shall have the meaning assigned to them hereunder:

2.1. 'Application' means all documents, information, statements and commitments submitted by the Licensee to CITC to request grant of this License.

2.2. 'Business address' means a dedicated, permanent and properly registered physical address, in which staff and/or an authorized representative of the Licensee is usually present and accessible during normal business hours.

2.3. 'Cloud Computing' means 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.

2.4. 'Cloud System' shall mean an electronic information system comprising hardware, software and networking elements owned, controlled or operated by a CSP to supply Cloud Services to Cloud Users.

2.5. 'Cloud Computing Service' (or 'Cloud Service') means an information and communications technology (ICT) service provided through Cloud Computing, which involves the storage, transfer or processing of User Content in a Cloud System. The mere storage and processing of customer 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..

2.6. 'Cloud User' means any Person making use of a CSP's Cloud Services. A Cloud User may also comprise multiple individuals or business units.

2.7. 'Licensed Service' means the service that the Licensee is licensed to provide under this License.

2.8. 'Residence' means a permanent or temporary residence in the Kingdom under the Kingdom's laws. It shall not include a temporary presence of persons transiting through the Kingdom.

2.9. 'User Address' means a Cloud User'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, User Address' shall mean that address.

2.10. 'Regulatory Framework' means the Regulatory Framework on Cloud Computing.

Article 2: Compliance with CITC Statutes and Decisions

1. The Licensee shall comply with the Commission Statutes including the Conditions of this License, the Telecommunications Act, its Bylaw, the Ordinance of CITC, and Regulatory Frameworks, Decisions and Guidelines issued from time to time by CITC.

2. The Arabic language version of the License shall be the official version and in case of any differences between the text of the official version written in the Arabic language and a translation into another language, the Arabic version shall prevail.

3. Licensee activities and behaviour shall be subject to the laws of the Kingdom.

Article 3: Grant of the License

1. Based on the Telecommunications Act, its Bylaws and the Ordinance of the Communications and Information Technology Commission, the Regulatory Framework on Cloud Computing and the Terms and Conditions of this License, CITC hereby issues this License to the Licensee to provide the services specified in Article 4 of this License.

2. The Licensee shall be bound by the information provided in its Application for this License.

Article 4: Scope of the License

1. The Licensee is hereby authorized to provide the following services in the entire territory of the Kingdom:

   1.1 Cloud Services to Cloud Users having a Residence or User Address anywhere in the territory of the Kingdom;

   1.2 Hosting of information and communications technology (ICT) equipment and services;

   1.3 Exercising direct or effective control over the processing and storing of User Content;

   1.4 Constructing and operating Datacentres and associated infrastructure for the provision of Cloud Services, directly or indirectly, through other, duly licensed or otherwise entitled, third parties;

   1.5 To the extent required for the provision of any of the Licensed Services authorized under paragraphs 1.1 to 1.4, above, connecting its infrastructure and network elements with any licensed Facility Based Provider or Internet Service Provider in the Kingdom.

2. Subject to paragraph 3, below, nothing in this License shall restrict the Licensee's right to provide duly licensed or approved Cloud Services similar to those licensed under this article or other services to users having a Residence or User Address outside the Kingdom.

3. The provisions of this License shall also be applicable with regard to any Cloud Service provided by the Licensee to Cloud Users other than those mentioned in paragraph 1.1, above, but only to the extent specified in Article 3.1.2 of the Regulatory Framework.

Article 5: General Obligations of the Licensee

The Licensee shall meet all the obligations stipulated in CITC Statutes and this License including continuity of providing the services and acting upon development and improvement of the services in accordance with CITC Statutes, and shall comply particularly with the following matters:

1. Implement and adhere to all policies, rules and instructions issued by CITC and other government bodies.

2. Behave with honesty and integrity.

3. Not discriminate between Cloud Users unless different terms are objectively justified.

4. All prices and features of the services to be provided must be clear to interested potential Cloud Users before their use.

5. Obtain the approval of the Chamber of Commerce in the area at which the Licensee is registered, if the service is connected directly or indirectly with providing a reward or a commercial promotion.

6. Not contradict the Islamic Sharia rules, good manners, morals, general rules or conventions and the public taste, and not do anything violating the Acts and Bylaws prevailing in the Kingdom.

7. Refrain from providing any services for which the Licensee does not have the appropriate license or other authorization, if any, that is required under the laws of the Kingdom.

8. Provide technical capabilities in its Datacentres, network equipment or any other devices as may be necessary to retain and identify Cloud Users' data relating to the Cloud Users' identity and usage, if this is needed under any applicable rules of the

Kingdom, for a minimum period of twelve (12) months or in accordance with CITC Statutes.

9. Obtain any other required approvals or authorizations from the relevant authorities prior to the start of service provision.

Article 6: Special Obligations of the Licensee

1. The Licensee shall have the rights and obligations set out in the following provisions of the Regulatory Framework:

1.1. Article 3.3 on information security including, without limitation, the rules applying to User Content classification and associated responsibilities, the transfer and location of user content, and the Licensee's obligations on the reporting of security breaches, information on its insurance coverage and obligations on internal rules and policies on business continuity, disaster recovery and risk management.

1.2. Article 3.4 on the protection of User Data including, without limitation, the applicable restrictions concerning the provision of User Content or User Data to third parties, and the rights of access, verification or deleting that the Licensee must grant to Cloud Users.

1.3. Article 3.5 on Unlawful Content and intellectual property including, without limitation, responsibilities regarding the presence and removal of Unlawful Content and User Content infringing intellectual property rights, and the protection of Cloud Users against third party claims for breaches of intellectual property rights.

1.4. Article 3.6 including, without limitation, the minimum mandatory content of the Licensee's Cloud Contracts with Cloud Users, dispute resolution procedures and the Licensee's obligations upon termination of the Cloud Contract.

1.5. Article 3.7 regarding consumer protection and unfair contract terms including, without limitation, certain restrictions of the Licensee's right to limit his liability.

1.6. Article 3.8 on quality, certification and standardisation including, without limitation, the Licensee's obligation to comply with any industry standards adopted as mandatory by CITC now or in the future.

Article 7: Information Requirements

1. The Licensee must have a Business Address in the Kingdom and an authorized representative with a Residence in the Kingdom and communicate in advance to CITC any related change.

2. This License shall be automatically terminated if the Licensee no longer meets any of its obligations under paragraph 1 above, and fails to remedy this, to the CITC's satisfaction, within thirty (30) calendar days of a request by the CITC.

3. The Licensee must submit any required information and/or periodic reports in accordance with the timeframe and format specified by CITC.

Article 8: License Effective Date

This License shall enter into force on its date of issue.

Article 9: License Amendment

CITC has the right to amend this License in accordance with CITC Statutes and for the benefit of the public.

Article 10: License Re-assignment and Subcontracting

1. Re-assignment of this License is subject to the provisions of Article 23 of the Telecommunications Act and its Bylaw.

2. The Licensee may, after obtaining prior written approval from the Commission, re-assign this License, provided that the re-assignee shall fulfil all legal, technical, financial and commercial requirements to obtain this License pursuant to CITC discretion and in compliance with its Statutes.

3. The Licensee is not permitted to contract with other persons to provide Licensed Services in accordance with this License without written approval from the Commission.

Article 11: License Revocation and Suspension

1. CITC may, at its sole discretion, revoke or suspend this License if the Licensee has committed any act requiring such revocation or suspension, and the Licensee alone shall be responsible for any and all liabilities resulting from such revocation or suspension, without any liability or responsibility being incurred by CITC.

2. The Licensee shall, if it intends to return the License, submit a written request to CITC three months prior to the date of stopping the licensed service.

3. The Licensee shall also settle all of its obligations with CITC and other parties, including its own Cloud Users.

Article 12: Violations & Penalties

Any violations and penalties relating to this License shall be dealt with in accordance with CITC Statutes.

Article 13: License Term and Renewal

This License shall be valid for 10 Hijra years from the date of issue. The License may be renewed for a similar period, subject to CITC approval in accordance with CITC Statutes at the time of renewal.

Article 14: Fees Payable by the Licensee

1. The Licensee shall pay to CITC the fees specified in Appendix 1 of this License.
2. CITC shall determine the process relating to the issuance of invoices and the method of payment with which the Licensee shall comply.
3. Payment shall be due immediately upon issuance of the invoice and shall be paid within one month of the invoice issuance date.

Appendix No. (1)

Fee Schedule for the Provision of Cloud Services

1. The Licensee shall pay the following fees in accordance with the terms of Article 14 of the License's Terms and Conditions:

   1.1. Commercial Provisioning Fee for the Licensed Services amounting to an annual payment of four percent 5% of Net Operating Income obtained from Cloud Users in the KSA;

   1.2. An annual fee against administrative work and services provided by CITC pursuant to its Statutes, that should be the maximum between 15,000 SAR and one percent 1% of Net Operating Income obtained from Cloud Users in the KSA.

2. 'Net Operating Income' in this Appendix means the total revenues received by the Licensee from providing the Licensed Services to Cloud Users with a Residence or Cloud Address in the KSA less any dues to any domestic and international service providers that are reflected in the settlement results of these services.

Annex D:
Draft Cloud Services License (CSL)

License Number:_____

Cloud Services License (CSL)

[Draft]

Issued to:

Company/Establishment:_____

Date of issue of this license __ /__ /____ (H) equivalent to __ /__ /____ (G)

Expiry date of this license __ /__ /____ (H) equivalent to __ /__ /____ (G)

Commercial Registration Number: _____

Date of issue of CR __ /__ /____ (H) Expiry date of CR: __ /__ /____ (H)

Issuing Location of CR: _____

Phone: _____ Fax: _____ Box: _____

Postcode: _____

Based on the Telecommunications Act issued by Royal Decree (M/12) dated 12/3/1422 and its Bylaws, and in accordance with the Communications and Information Technology Commission ('CITC') Ordinance issued under the Council of Ministers Decision No. (74) dated 5/3/1422, CITC has issued this License to the company/establishment above in accordance with the following conditions and annexes which together comprise integral parts of this License:

- License Terms & Conditions
- Appendix (1) Fee Schedule

Official Seal

Table of Contents

Article 1: Definitions

1. The words and expressions defined in the Telecommunications Act, its Bylaws, the Ordinance of the Communications and Information Technology Commission ('CITC') and the Regulatory Framework on Cloud Computing shall have the same meanings in this License.

2. The following words and expressions shall have the meaning assigned to them hereunder:

2.1. 'Application' means all documents, information, statements and commitments submitted by the Licensee to CITC to request grant of this License;

2.2. 'Address for Service' means an address for the valid delivery to the Licensee, under the laws of the Kingdom, of any notices or other legal documents;

2.3. 'Cloud Computing' means 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.

2.4. 'Cloud System' shall mean an electronic information system comprising hardware, software and networking elements owned, controlled or operated by a CSP to supply Cloud Services to Cloud Users.

2.5. 'Cloud Computing Services' (or 'Cloud Services') means information and communications technology (ICT) services provided through Cloud Computing, which involve the storage, transfer or processing of User Content in a Cloud System. The mere storage and processing of customer 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.

2.6. 'Cloud User' means any Person making use of a CSP's Cloud Services. A Cloud User may also comprise multiple individuals or business units.

2.7. 'Licensed Services' means the services that the Licensee is licensed to provide under this License.

2.8. 'Residence' means a permanent or temporary residence in the Kingdom under the Kingdom's laws. It shall not include a temporary presence of persons transiting through the Kingdom.

2.9. 'User Address' means a Cloud User'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, User Address' shall mean that address

2.10. 'Regulatory Framework' means the Regulatory Framework on Cloud Computing.

Article 2: Compliance with CITC Statutes and Decisions

1. The Licensee shall comply with the Commission Statutes including the Conditions of this License, the Telecommunications Act, its Bylaw, the Ordinance of CITC, and Regulatory Frameworks, Decisions and Guidelines issued from time to time by CITC .

2. The Arabic language version of the License shall be the official version and in case of any differences between the text of the official version written in Arabic language and a translation into another language, the Arabic version shall prevail.

3. Licensee activities and behaviour shall be subject to the laws of the Kingdom .

Article 3: Grant of the License

1. Based on the Telecommunications Act, its Bylaws and the Ordinance of the Communications and Information Technology Commission, the Regulatory Framework on Cloud Computing and the Terms and Conditions of this License, CITC hereby issues this License to the Licensee to provide the services specified in Article 4 of this License.

2. The Licensee shall be bound by the information provided in its Application for this License.

Article 4: Scope of the License

1. The Licensee is hereby authorized to provide Cloud Services to Cloud Users having a Residence or User Address anywhere in the territory of the Kingdom.

2. The Licensed Services do not include, in particular, any of the following services or activities:

   2.1. Hosting of information and communications technology (ICT) equipment and services in the Kingdom;

   2.2. Exercising direct or effective control over the processing and storing of User Content that qualifies as Level 3 User Content, as this term is determined pursuant to Article 3.3. of the Regulatory Framework;

   2.3. Constructing and operating Datacentres and associated infrastructure in the Kingdom for the provision of Cloud Services, directly or indirectly, through other duly licensed or otherwise entitled third parties.

3. Nothing in this License shall restrict the Licensee's right to provide duly licensed or approved Cloud Services similar to those licensed under this article or other services to Cloud Users having a Residence or User Address outside the Kingdom. The provisions of this License shall not apply to any such services by the Licensee outside the Kingdom.

Article 5: General Obligations of the Licensee

The Licensee shall meet all the obligations stipulated in CITC Statutes and this License including continuity of providing the services and acting upon development and improvement of the services in accordance with CITC Statutes, and shall comply particularly with the following matters:

1. Implement and adhere to all policies, rules and instructions issued by CITC and other government bodies.

2. Behave with honesty and integrity.

3. Not discriminate between Cloud Users unless different terms are objectively justified.

4. All prices and features of the services to be provided must be clear to interested potential Cloud Users before their use.

5. Not contradict the Islamic Sharia rules, good manners, morals, general rules or conventions and the public taste, and not do anything violating the Acts and Bylaws prevailing in the Kingdom.

6. Refrain from providing any services for which he does not have the appropriate license or other authorization, if any, that is required under the laws of the Kingdom.

7. Obtain any other required approvals or authorizations from the relevant authorities prior to the start of service provision.

Article 6: Special Obligations of the Licensee

1. The Licensee shall have the rights and obligations set out in the following provisions of the Regulatory Framework:

   1.1. Article 3.3 on information security including, without limitation, the rules applying to User Content classification and associated responsibilities, the transfer and location of user content, and the Licensee's obligations on the reporting of security breaches, information on his insurance coverage and obligations on internal rules and policies on business continuity, disaster recovery and risk management.

   1.2. Article 3.4 on the protection of User Data including, without limitation, the applicable restrictions concerning the provision of User Content or User Data to third parties, and the rights of access, verification or deleting that the Licensee must grant to Cloud Users.

   1.3. Article 3.5 on Unlawful Content and intellectual property including, without limitation, responsibilities regarding the presence and removal of Unlawful Content and User Content infringing intellectual property rights, and the protection of Cloud Users against third party claims for breaches of intellectual property rights.

1.4. Article 3.6 including, without limitation, the minimum mandatory content of the Licensee's Cloud Contracts with Cloud Users, dispute resolution procedures and the Licensee's obligations upon termination of the Cloud Contract.

1.5. Article 3.7 regarding consumer protection and unfair contract terms including, without limitation, certain restrictions of the Licensee's right to limit his liability.

1.6. Article 3.8 on quality, certification and standardisation including, without limitation, the Licensee's obligation to comply with any industry standards adopted as mandatory by CITC now or in the future.

Article 7: Information Requirements

1. The Licensee must have a valid Address for Service in the Kingdom and must communicate any change in advance to CITC.

2. The Licensee must communicate in advance to CITC any change of its business address.

3. The Licensee must submit any required information and/or periodic reports, for statistical purposes, in accordance with the timeframe and format specified by CITC.

Article 8: License Effective Date

This License shall enter into force on its date of issue.

Article 9: License Amendment

CITC has the right to amend this License in accordance with CITC Statutes and for the benefit of the public.

Article 10: License Revocation and Suspension

1. CITC may, at its sole discretion, revoke or suspend this License if the Licensee has committed any act required such revocation or suspension, and the Licensee alone shall be responsible for any and all liabilities resulting from such revocation or suspension, without any liability or responsibility being incurred by CITC.

2. The Licensee shall, if it intends to return the License, submit a written request to CITC three months prior to the date of stopping the service.

3. The Licensee shall also settle all of its obligations with CITC and other parties, including Cloud Users.

Article 11: Violations & Penalties

Any violations and penalties relating to this License shall be dealt with in accordance with CITC Statutes.

Article 12: License Term and Renewal

This License shall be valid for one (1) Hijra year from the date of issue. The License may be renewed for a similar period, subject to CITC approval in accordance with CITC Statutes at the time of renewal.

Article 13: Fees Payable by the Licensee

1. The Licensee shall pay to CITC the fees specified in Appendix 1 of this License.
2. CITC shall determine the process relating to the issuance of invoices and the method of payment with which the Licensee shall comply.
3. Payment shall be due immediately upon issuance of the invoice and shall be paid within one month of the invoice issuance date.

Appendix No. (1)

Fee Schedule for the Provision of Cloud Services

1. The Licensee shall pay the following fees in accordance with the terms of Article 13 of the License's Terms and Conditions:

   1.1. Commercial Provisioning Fee for the Licensed Services amounting to an annual payment of 5,000 SAR.

   1.2. An annual fee of 5,000 SAR against administrative work and services provided by CITC pursuant to its Statutes.

Annex E:
Draft Cloud Services Declaration

Cloud Services Declaration (CSD)

[Draft]

1. Information on the Declarant

Name of Company or Corporation (in Arabic), if applicable: .....

CR No: .....

Name of Company or Corporation (in English): .....

Address of registered seat or main place of business:

.....

.....

.....

.....

Tel: .....

Fax: .....

Website: .....

Name of Signatory:.....

Position:.....

Professional address:.....

.....

.....

Tel (fixed): .....

Tel (mobile): .....

Fax: .....

email: .....

Name of a Contact Person (if other than the Signatory)

.....

Position:.....

Professional address:.....

.....

.....

Tel (fixed): .....

Tel (mobile): .....

Fax: .....

email: .....

Address for service in the KSA:

.....

.....

.....

.....

Tel: .....

Fax: .....

2. Information on the Declarant's Activities

Please provide a brief description of the type of cloud service(s) you plan to provide or are providing already to cloud users with a residence or user address in the KSA, and the technical means (cloud system, networking elements, etc.) relied upon for the provision of these services.
Please provide a list of any licenses held to date in the KSA, granted by CITC to (i) the Declarant, (ii) any affiliate of the Declarant or (iii) any joint venture in which the Declarant or an affiliate of the Declarant participates.

3. Commitments by the Declarant

I, the undersigned, acting for and on behalf of ..... ('the Declarant') acknowledge, certify and agree that:

- the information provided in this Declaration and its attachments is true and correct;
- the Declarant shall comply with the terms and conditions of the Regulatory Framework the Guidelines, and any applicable CITC statutes, as well as any future amendments to the above;
- the Declarant shall extend, not later than one month from the effective date of this Declaration, its terms and conditions to its existing cloud users (if any) with a residence or user address in the Kingdom;
- the Declarant shall inform CITC immediately of any changes to the information provided under heading (1) above ('Information on the Declarant');
- the Declarant accepts that CITC may publish any of the information provided by the Declarant in this Declaration except any such information reasonably qualifying as a confidential business secret, provided that the Declarant has identified this information in a separate attachment to this Declaration and has provided an explanation, to CITC's reasonable satisfaction, of the reasons why it should not be disclosed to the public.

_____ _____

Name, Title and Signature Place and Date

هيئة الاتصالات وتقنية المعلومات السعودية
www.citc.gov.sa info@citc.gov.sa
199099 0114618000