CITRA

الهيئة العامة للاتصالات وتقنية المعلومات

COMMUNICATION & INFO. TECHNOLOGY REGULATORY AUTHORITY

Cloud Service Providers Regulations and Commitments

State of Kuwait

V1.7

Communication and Information Technology Regulatory Authority

Table of Contents

Introduction

Under its establishment law No. 37 of 2014 and amended by law No. 98 of 2015 the Communication and Information Technology Regulatory Authority (CITRA) is authorized to issue regulations, policies and regulatory guidelines for the telecommunication and information technology sectors to achieve comprehensive development in the State of Kuwait.

CITRA initiated this document to implement the Cloud Regulatory Framework regulations, and to detail the commitments, and registration regulations of Cloud Service Providers (CSPs) who are wishing to provide these services in the State of Kuwait to host Tier 3 and Tier 4 data, and to get the required license from CITRA.

Furthermore, entities that use Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) cloud models, from Cloud Service Providers (CSPs), that host data from the first and second tiers (Tier 1 and Tier 2), shall direct these CSPs to register and obtain a permission from CITRA (or obtain a permission by registering on CITRA's website).

This document appends Cloud Regulatory Framework, support and is in line with Cloud First Policy and Data Classification Policy.

Hereby, CITRA announces that service providers are prohibited from signing any contracts to provide cloud services to the public sector in the State of Kuwait, until registering and obtaining a permission/or a license from CITRA and complying with all the commitments stated in the Cloud Regulatory Framework document and this document.

Definitions

The following terms and expressions, wherever mentioned in this document, shall have the meanings assigned to them below. The definitions mentioned in the Communication and Information Technology Regulatory Authority Law No. 37 of 2014 and as amended by Law No. 98 of 2015, its executive regulations, ICT Terms and Definitions, Cloud Regulatory Framework, Data Classification Policy, and Cloud First Policy issued by the authority are all adopted.

Registration and Permission: it is designated for cloud service providers (CSPs) that host the tier 1 and tier 2 of data classification, to register on CITRA's website to comprehend and comply with the commitments stipulated in this document.

License: the permit under which CITRA grants permission to the cloud service providers to provide Software-as-a-Service (SaaS), or Platform-as-a-Service (PaaS) or Infrastructure-as-a-Service (IaaS) operating within the State of Kuwait.

Data Center: is an administration within an entity/organization that hosts and maintains its back-end information technology systems, data storage, computers, servers, and databases. In times of large central IT operations, this administration and all its systems are in one place called the data center.

Service Organization Control 2 (SOC Type II): is an auditing procedure to ensure that service providers manage subscribers' data, while complying with security regulations to protect the subscribers' interests and their data privacy concerns. This procedure must be adhered to when a subscriber wishes to buy Software-as-a-Service (SaaS) from a cloud service provider.

Cloud Controls Matrix: is a cloud cybersecurity framework consisting of 133 control tools spread over 16 domains to cover the basic elements of cloud technology. This framework was created by the Cloud Security Alliance (CSA).

Cloud Security Alliance (CSA): A non-profit organization that aims to promote the use of best practices to ensure cloud security.

Regulatory Authorities: entities responsible for governing, monitoring and regulating work procedures in government entities and/or private companies in the State of Kuwait, and have the authority to issue policies and regulations within its domain and in accordance with a decree, law or a mandate from the Council of Ministers.

Cloud Service Providers and Subscribers Commitments and Responsibilities

The Cloud Regulatory Framework illustrated the cloud service models provided by the cloud service providers. The service provider's and the subscriber's commitments and responsibilities vary depending on the provided service model (Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS)) as follows:

1. Infrastructure-as-a-Service (IaaS):

In this model, The Cloud Regulatory Framework illustrated that the service provider hosts the infrastructure components, and the subscriber does not manage or control the main cloud infrastructure but rather manages the operating system, storage, applications and some protection systems.

Therefore, the service provider's commitments and responsibilities who wishes to provide the infrastructure as a service (IaaS) are detailed as follows:

1. The service provider commits to provide, protect, secure, maintain the availability, and manage the infrastructure components that constructs a data center (servers, network devices, storage, and virtualization layer) for the cloud environment according to the standards mentioned in the Cloud Regulatory Framework.
2. The service provider commits to provide necessary technical support to the subscriber, as well as ensuring that their cloud environment suits the subscriber's needs and requirements.

2. Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS) or Both:

The Cloud Regulatory Framework illustrated that in a Platform-as-a-Service (PaaS) model, the service provider provides the environment that includes both hardware and software tools required to develop applications for the subscribers over the internet. The service provider hosts the hardware and software on its own infrastructure, thus exempting subscribers from purchasing infrastructure to install ICT solutions.

Moreover, the Framework illustrated that the Software-as-a-service (SaaS) model is a software distribution model in which a service provider hosts applications and makes them available to subscribers via the Internet.

Therefore, commitments and responsibilities of the service provider who wishes to provide platform-as-a-service (PaaS), or software-as-a-service (SaaS), or both are detailed as follows:

1. The service provider commits to provide, protect, secure, maintain the availability, and manage the infrastructure components that constructs a data center (servers, network devices, storage, and virtualization layer) for the cloud environment according to the standards mentioned in the Cloud Regulatory Framework.
2. The service provider commits to provide necessary technical support to the subscriber, as well as ensuring that their cloud environment suits the subscriber's needs and requirements.
3. The service provider commits to manage and protect operating systems and databases.
4. The service provider commits to help subscribers comply with privacy and personal data protection laws by providing sufficient technical and regulatory measures to protect the subscriber's data and content on cloud platforms, as well as meeting security and protection requirements requested by the subscriber based on the subscriber's data and content classification levels.
5. The service provider that gathers personal information from their subscribers commits to create a clear and easily accessible privacy policy that guarantees the provider's and subscribers' rights in accordance with the laws, regulations and procedures that are enforced in the state of Kuwait. It should include:

   5.1 Types of personal information gathered from subscribers:

   5.1.1 The service provider has no right to request "special categories of personal data" (which were defined in the Cloud Regulatory Framework) from subscribers.

   5.1.2 The service provider commits to clarify to the subscribers all matters related to the personal identity data, which the subscribers provide to the service provider directly or indirectly, and the data that the service provider gathers from the subscribers or the data that is gathered automatically.

5.1.3 The list of information that a service provider gathers directly may include, but is not limited to, the following:

5.1.3.1 Name and Email address

5.1.3.2 Address

5.1.3.3 Credit Card or Payment Information

5.1.3.4 IP address and location

5.1.3.5 Use of Products and Services

5.1.3.6 Device and Browser Information

5.1.4 The following are some examples of information that a service provider may gather automatically:

5.1.4.1 IP Address

5.1.4.2 The subscriber's geographical location

5.1.4.3 Subscriber's Preferences

5.1.4.4 Computer, browser, and software information

5.1.4.5 Subscriber's activities date and time

5.2 Personal data collection and usage mechanism

5.2.1 After specifying the types of gathered data, the service provider commits to explain to the subscriber how the data was collected, whether it was through online forms or other automated procedures.

5.2.2 The service provider commits to provide the reasons for collecting this data to the subscribers and the importance of its uses.

5.3 The methods used for protecting the subscribers' personal information.

5.4 Subscribers' rights regarding their information.

5.5 Cookies Used: Cookies have become a popular tool for companies to track how subscribers interact with their websites and mobile applications. Since this technology contributes to understanding customer "behavioral data" in browsing, searching for, and buying products; it also comes with privacy risk. Since some cookies continue to track users' activity even after they leave the company's website or mobile application, the following commitments fall on the service provider:

5.5.1 The service provider commits to state a clear clause in its privacy policy called "Cookies", explaining, and defining their uses and reasons for its use according to the usage classifications in the mechanism of:

5.5.1.1 Login Authentication

5.5.1.2 Security inferences

5.5.1.3 Advertisements

5.5.1.4 The subscriber's personal preferences for the service provider to provide real-time information or services as defined in the "personal identification" definitions mentioned in the Cloud Regulatory Framework.

5.5.2 The service provider is prohibited to use these types of data to infer the identity of subscribers.

5.5.3 The service provider commits to provide subscribers with a full list that contain each type of cookies used by its website or mobile application, in addition to the cookies used by external parties (third parties).

5.6 Third-party information: The service provider must inform subscribers that they have applications/systems that operates as a third party to perform certain services on a website or mobile application. Some examples are, but not limited to, Google AdSence, identity management programs, and others, as well as privacy policies of these applications/systems/services if available to maintain transparency.

5.6.1 The service provider commits not to share or sell the data to any party. Third party access may be granted to personal data including name, address, phone number, and e-mail for the purpose of improving the service and user experience.

5.6.2 The subscriber must be notified if their data to be transferred due to enterprise acquisitions, liquidation, or any dissolution.

5.6.3 The third party must disclose data to the security authorities in the following cases:

5.6.3.1 To adhere to any applicable law, regulation, legal process, or governmental request enforced within the borders of the State of Kuwait.

5.6.3.2 Detect, prevent or address occurring fraud, security or technical problems.

5.6.3.3 To provide protection and defend rights, possessions or the safety of government entities or subscribers as required or permitted by the laws of the State of Kuwait.

5.6.4 The Subscriber has the right to request amendment or the deletion of their personal data available to third parties.

5.7 Conditions of data retention: The service provider must clarify the following in their privacy policy:

5.7.1 Where data is stored and how subscribers can access it to view its details or amend it.

5.7.2 The mechanism that grants subscribers the right to delete, cancel or amend their data.

5.7.3 The mechanism that grants the service provider the right to delete the subscribers' data in the event of non-compliance with the requirements of service providers.

5.7.4 The mechanism which indicates the necessity to keep some subscribers' data such as application/system history usage or unpaid dues.

5.8 Communication: The service provider's privacy policy must include:

5.8.1 The communication channels with the subscribers (email, text messages, etc.), whether if they are for marketing, billing, or notifications.

5.8.2 The mechanism that enables the subscriber to cancel marketing communications subscription.

5.9 Change of ownership: In the event of changing of ownership by acquisition, purchase or merger, the service provider must inform subscribers immediately that their personal data will be transferred to the new owners.

5.10 The service provider, who provides Software-as-a-Service model, must clarify in their privacy policy the targeted age group. If the targeted age group are minors, the following applies:

5.10.1 A parental (or legal guardian) consent must be obtained. Common methods can be used to obtain this consent, such as billing the credit card of the parent (or legal guardian) with a token amount not exceeding twenty fils (20 fils) to verify the consent of the parent/legal guardian, or by sending a web-link that uses the

parent's/legal guardian's approved digital ID and E-signature by the Public Authority for Civil Information (PACI) for consent verification.

5.10.2 Specify services (or specifications) not to be used by this group, some examples are but not limited to chat rooms, purchasing, or changing the settings on the service provider's website.

5.10.3 Consider Child Protection Law or any laws, regulations or amendments enforced or to be issued later in the State of Kuwait.

5.11 Changes to the Privacy Policy: The service provider has the right to amend its privacy policy according to procedures that do not conflict with the laws and regulations enforced in the State of Kuwait, provided that the service provider will notify the subscribers about these changes.

5.12 Communication: The service provider commits to put in place a clear and a specific mechanism that enables the subscriber to communicate with the service provider regarding the subscriber's data privacy.

6. The service provider shares the following responsibilities with the subscriber:

6.1 Responsibility to determine access controls, user creation, and granting authorizations that allow users to edit, process or transfer the subscriber's data and content.

6.2 Responsibility to manage applications and software control tools.

6.3 The service provider can share the network management control tools with the subscriber, should the subscriber request it.

3. Service Providers Who Provide More Than One Service Model

Cloud service providers may wish to provide more than one service model, or all the cloud services discussed above; in that case, all commitments related to each service to be provided by the cloud service provider applies.

Cloud Service Providers General Regulations

1. Comply with the Cloud Regulatory Framework, its related policies, and laws enforced in the State of Kuwait.

2. Must register with CITRA to be eligible for privileges related to obtaining a permission or a license based on what is stipulated in the Cloud Regulatory Framework and this document.
3. Commits to assist subscribers to comply with privacy and individual's personal data protection laws by demonstrating adequate technical and regulatory measures to protect entities and companies' data on cloud platforms.
4. Commits to comply with the regulations mentioned in the previous chapter regarding cloud service models that they provide without violating any regulations stated in the Data Classification Policy and in the Cloud Regulatory Framework that relates to subscribers' personal data and governmental or institutional data.
5. Cloud service providers should assist subscribers to comply with the requirements of the regulatory authorities in the State of Kuwait, such as CITRA or external auditors by creating auditing records and sharing them with a high level of transparency.
6. Fully comply with the State of Kuwait laws and regulations, whether issued by CITRA or other governmental entities, regarding information technology, data protection and privacy, cybercrime, as well as what is stated in Law No. 20 regarding electronic transactions, contracting, and any other regulations or laws that get issued in the future.
7. Complies with the Data Classification Policy and Cloud First Policy issued by the Communication and Information Technology Regulatory Authority (CITRA), and with the cybersecurity standards for cloud computing issued by the authority, in addition to any related policies, regulations or instructions issued by the authority.
8. Telecommunication companies and Internet Service Providers (ISPs) must commit and comply with the cloud Regulatory Framework, and the relevant policies and regulations issued by CITRA in addition to service providers' commitments mentioned in this document and must obtain CITRA's approval to provide cloud services to subscribers.
9. It is within the Communication and Information Technology Regulatory Authority (CITRA) jurisdiction to amend the registration and licensing regulations without prior notice.

Registration and Permission Procedure

Communication and Information Technology Regulatory Authority (CITRA) specifies the registration procedure for cloud service providers, who host Tier 1 and Tier 2, to obtain a permission as follows:

1. Fill the necessary service provider identification information on the permission form on CITRA's website.
2. State the type(s) of service(s) to be provided to subscribers.
3. Agree to the regulations and conditions on the permission form available on CITRA's website, which were mentioned above in this document, in the chapter "Cloud Service Providers Commitments and Responsibilities" Clause No. 2 "Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS) or both", Point No. 5 related to the service provider's privacy policy.

Licensing Procedure

Cloud service providers wishing to host Tier 3and Tier 4 data are required to provide CITRA with information, identifications, certificates, and documents that are listed in the articles below to complete their registration process and obtain their license from CITRA as accredited cloud service providers. Service Providers are prohibited from providing cloud services to the public or private sectors prior to obtain this license.

1. Submit identification documents from the related entities in Kuwait.
2. Submit supporting documents which prove that the cloud service provider operates and owns a licensed data center(s) by the related entities in the country and is located within the Kuwaiti borders. The data center(s) must include(s) infrastructures and operating platforms designated to host cloud environments fully or partially, through which, the service provider intends to provide full or partial cloud services.
3. Provide CITRA with the owned data center(s) technical and non-technical specifications documents. The technical specifications must include data center classification (Tier 1, Tier 2, Tier 3), available equipment and devices, and the applied security and protection standards.

4. Commits to disclose the following to CITRA:
   4.1 Other service providers jointly co-hosting the cloud environment fully or partially on its owned data center.
   4.2 The geographical locations, addresses, contact information, and the primary characteristics of any owned data center within Kuwait's boarders.
   4.3 The list of countries (or county) which the service provider owns data centers in, if these data centers are used to process, transit, or transmit contents owned by a subscriber residing in Kuwait (i.e. has a Kuwaiti address).
5. Submit documents to specify the type of cloud services the provider wishes to provide ((Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS)), the type of the available cloud operating environment, and the cloud deployment models (public, private, community, or hybrid).
6. Submit documents that show targeted subscribers' type(s), whether these subscribers reside in or outside Kuwait (individuals, government entities, and companies in the private sector).
7. Submit documents to prove enterprise-level partnership(s) with one or more global cloud service providers and competency certifications from them, if the service provider wants to provide the services offered by these global service providers as a broker (middleman) or services aggregator.
8. Service providers who were and still providing cloud services prior to and when the Cloud Regulatory Framework, its associated policies and regulations, and this document are issued and enforced, must correct their status by:
   8.1 Open data centers referenced in Point No. 2 above and obtain the required licenses.
   8.2 Obtain the license to provide cloud services in Kuwait from CITRA in accordance with the general regulations and licensing procedures mentioned in this document.
   8.3 Service providers are given a period of six months (6 months) from the issuance date of the Cloud Regulatory Framework, its associated policies, and regulations to correct their status as mentioned above.
   8.4 All contracts between cloud service providers with subscribers will be voided, if the service providers do not get the license within the period mentioned above.

9. CITRA has the right to impose penalties and fines on the service providers, as it sees fit, in the event they do not obtain the licenses mentioned above.
10. In addition to the document mentioned above, the service provider can submit any other supporting documents.
11. CITRA will review all submitted documents by the service provider, and if all the conditions are met, CITRA will issue the necessary license.
12. CITRA has the right to exclude or refuse to license a service provider without providing any justifications as it deems appropriate.
13. The license is valid for one year from the date of issuance, and the service provider must renew this license annually by submitting all the documents to CITRA.

Related Documents

The documents listed below (with their appendices) are related to this guide and can be reviewed through Communication and Information Technology Regulatory Authority's (CITRA's) official website: (www.citra.gov.kw)

1. Cloud First policy
2. Data Classification Policy
3. ICT Terms and Definitions