REPUBLIC OF THE PHILIPPINES

DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

18 January 2017

DEPARTMENT CIRCULAR
NO. 2017 - **002**

TO: **ALL HEADS OF DEPARTMENTS, BUREAUS, OFFICES AND OTHER AGENCIES OF THE NATIONAL GOVERNMENT, INCLUDING CONSTITUTIONAL COMMISSIONS, CONGRESS, THE JUDICIARY, OFFICE OF THE OMBUDSMAN, STATE UNIVERSITIES AND COLLEGES, GOVERNMENT-OWNED OR -CONTROLLED CORPORATIONS, LOCAL GOVERNMENT UNITS AND ALL OTHERS CONCERNED**

SUBJECT: **PRESCRIBING THE PHILIPPINE GOVERNMENT'S CLOUD FIRST POLICY**

SECTION 1. BACKGROUND AND RATIONALE

1.1 Section 2(b) of Republic Act No. 10844 (R.A. 10844) declared as a policy of the state to ensure the provision of a strategic, reliable, cost-efficient and citizen-centric information and communications technology infrastructure (infostructure), systems and resources as instruments of good governance and global competitiveness.

1.2 Section 6(I)(a) of R.A. 10844 provided the Department of Information and Communications Technology (DICT) the power to formulate, recommend and implement national policies, plans, programs and guidelines that will promote the development and use of ICT with due consideration to the advantages of convergence and emerging technologies.

1.3 Section 6(III)(f) of R.A. 10844 also provided the DICT the responsibility to harmonize and coordinate all national ICT plans and initiatives to ensure knowledge, information and resource-sharing, database-building and agency networking linkages among government agencies, consistent with E-Government objectives in particular, and national objectives in general.

SECTION 2. PURPOSE

This Department Circular is being issued to prescribe the Philippine government policy on reducing the cost (acquisition and operation) of government ICT by eliminating the duplication of hardwares and systems, fragmentation of databases and the use of cloud computing technology to reduce costs, increase employee productivity and develop excellent citizen online services.

SECTION 3. COVERAGE

3.1 This Department Circular shall cover all Departments, Bureaus, Offices and Other Agencies of the National Government, including Constitutional Commissions, Congress, the Judiciary, Office of the Ombudsman, State Universities and Colleges, Government-Owned or -Controlled Corporations and Local Government Units.

3.2 The implementation of this Department Circular shall also cover private entities that will participate as accredited cloud service providers.

SECTION 4. DEFINITION OF TERMS

4.1 **What is cloud computing?**

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five (5) essential characteristics, five (5) deployment models and certain assurances.

4.2 **Essential Characteristics of Cloud Computing**

On-demand Self-service. Government agencies can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad Network Access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, tablets, laptops and workstations).

Resource Pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to agency demand. There is a sense of location independence in that the government agency generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g. country, state, or datacenter). Examples of resources include storage, processing, memory and network bandwidth.

Rapid Elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the agency, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured Service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g. storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both the provider and consumer (i.e., the government agency) of the utilized service.

4.3 Deployment Models of Cloud Computing

Private. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g. government agencies). It may be owned, managed and operated by the organization or a third party and it may exist on or off premises.

Virtual Private. The cloud infrastructure is provisioned for exclusive use by a single organization based on enhanced global security and compliance standards. It provides a virtual private cloud environment off premise with strong isolation and may provide dedicated infrastructure for exclusive use by an organization.

Community. The cloud infrastructure is provisioned for exclusive use by a specific community of users from agencies (or organizations) that have shared concerns (e.g. mission, security requirements, policy and compliance considerations). It may be owned, managed and operated by one or more of the agencies in the community, a third party or some combination of them and it may exist on or off premises.

Public. The cloud infrastructure is provisioned for open use. It may be owned, managed and operated by a business, academic or government organization or some combination of them. It exists on the premises of the cloud provider.

Hybrid. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g. cloud bursting for load balancing between clouds).

Government Cloud (also known as GovCloud). A public service cloud infrastructure provisioned by the DICT for use by government agencies. GovCloud is a hybrid deployment of on-premise resources controlled and provisioned by DICT and as well as resources from accredited Cloud Service Providers (CSPs). Eligible CSPs must be pre-accredited to provide services to all Departments, National Government Agencies and Government-Owned and Controlled-Corporations (GOCCs), including State Universities and Colleges (SUCs). To be accredited, CSPs must meet a specific minimum set of standards for providing services to government agencies and this accreditation process will be managed by the DICT.

4.4 Assurance Approaches

Shared Responsibilities – Security and compliance responsibilities in developing cloud systems are shared between the Cloud Service

Provider (CSP) and the government agency. The level of responsibility on both parties depends on the cloud deployment model type and agencies should be clear as to their responsibilities in each model.

SECTION 5. CLOUD FIRST POLICY

5.1 Cloud computing has brought a new and more efficient means of managing government information technology resources. It is hereby declared the policy of the government to adopt a "cloud first" approach and for government departments and agencies to consider cloud computing solutions as a primary part of their infostructure planning and procurement.

5.2 All government agencies shall adopt cloud computing as the preferred ICT deployment strategy for their own administrative use and delivery of government online services, except:

5.2.1 When it can be shown that an alternative ICT deployment strategy meets special requirements of a government agency; and

5.2.2 When it can be shown that an alternative ICT deployment strategy is more cost effective from a Total Cost of Ownership (TCO) perspective and demonstrates at least the same level of security assurance that a cloud computing deployment offers.

SECTION 6. BENEFITS DERIVED FROM THE USE OF CLOUD COMPUTING TECHNOLOGY

6.1 **Inter-Agency Collaboration for Greater Efficiency and Better Citizen Online Services** – Cloud computing enables more effective collaboration as agencies are able to easily share resources across institutions, allowing for greater efficiency, entrepreneurship and creativity in delivering public online services.

6.2 **Operational Continuity and Business Recovery** – With centralized data storage, management and backups, data retrieval and business recovery during times of crisis (e.g. natural disasters or other disruptive events) become faster, easier and more cost effective.

6.3 **Faster Deployment of Services** – Reducing the amounts of infostructures required to be built and owned by government agencies reduces overall deployment times and shifts the focus from management of infrastructure to delivery of online services. Public ICT facilities and services can be tested and deployed quicker and maintained more cost effectively than if the government agencies will own and run unique computing facilities themselves.

6.4 **Greater Budget Control** – A utility-based "pay for what you use" model means that government agencies can purchase as much or as little resources as they need it. Cloud scalability results in systems usage being dialed up or down throughout the year as it is required. Transparency of the utility-based pricing structure means that spending caps and alerts can be implemented to further assist in budget control.

6.5 **Decreased Spending on Legacy Infrastructure** – Deploying government online services in cloud infrastructure results in immediate reductions of large capital outlays for infostructure and maintenance costs. More commodity solutions – including best of class services – are also made available to government agencies through cloud provisioning. The cloud first model enhances government ICT resiliency and security as version upgrades to both hardware and software are managed by the cloud service provider.

SECTION 7. ROLE OF DICT'S GOVCLOUD

7.1 The initial GovCloud infrastructure was set up in 2013 by DOST-ICT Office as part of the Integrated Government Philippines (iGovPhil) Project which aims to provide cloud infrastructure access to government agencies. As the public sector adopts a cloud first policy, the Philippine GovCloud will continue to support agencies efforts to adopt cloud solutions according to their requirements.

7.2 In order to expand and fulfill cloud service requirements in the public sector, DICT will be developing a list of accredited cloud service providers. Together with on-premise resources from the DICT, this set of accredited CSPs is hereby referred to as the new version of

GovCloud. The process for accreditation into the new GovCloud is detailed in **SECTION 15. ACCREDITATION PROCESS FOR CSPs** of this Circular.

SECTION 8. BENEFITS OF MAINTAINING PRE-ACCREDITED GOVCLOUD VENDORS

8.1 **Saves time.** By leveraging a pre-accredited list, Philippine Government agencies are able to streamline cloud computing tender processes involving only pre-accredited providers, as opposed to having agencies undertake individual assessments of cloud service providers for each tender or develop their own datacenters or on-premises cloud facilities.

8.2 **Ensures quality.** The pre-accredited list of cloud vendors would have been pre-vetted to ensure their services meet or exceed the mandatory security controls for government cloud usage.

8.3 **Ensures compliance.** The operations of the new GovCloud are governed by the laws of the Republic of the Philippines. All contracts, agreements, and service level agreements pertaining the same are bound by Philippine laws and any claims or issues raised shall be resolved in the Philippine courts or Philippine adjudicatory bodies.

SECTION 9. DATA CLASSIFICATIONS

9.1 Classifying data into discrete categories enables the Philippine Government to better protect government information and make better-informed decisions with regard to access, storing and transmission of Government data. Data classifications achieve stronger outcomes for government agencies by clarifying the safeguards required for protecting different types of data, thereby reducing uncertainty, standardizing access and reducing costs. It also enables business and other public sector agencies to be able to better use and manage appropriately classified data.

9.2 For purposes of this policy document, data can be broadly divided into three tiers of Public Sector Data Classification:

Tier 1: **Non-sensitive or Unclassified Data,** which can be stored on accredited public cloud or the Philippine GovCloud;

Tier 2: **Restricted or Sensitive Data**, which can be stored on accredited public cloud or the Philippine GovCloud, with encryption requirements; and

Tier 3: **Confidential or above-Sensitive Data**, which may require private (on premise) cloud deployment with specific encryption requirements.

9.3 Government agencies are recommended to select the appropriate cloud deployment model according to an agency's specific needs and the type of data it handles according to the Public Sector Data Classification, as illustrated in the table below. Depending on the classification of the agency's data, there will be a requirement to apply certain controls. Agencies may find that these controls are addressed by a public cloud provider or that they may only be serviced by a private cloud delivered on-premise.

Public Sector Data Classification	Suggested Cloud Deployment Model	Data Examples	M.C. 78, s1964 Correspondence
Tier 1: Non-sensitive or Unclassified Data	Can be stored on accredited public cloud or Philippine GovCloud.	Open Data, publicly available information including informational websites, terminology systems, standards, practitioner registries	• Non-sensitive Matters
Tier 2: Restricted Sensitive Data	Can be stored on accredited public cloud or GovCloud and meets a higher set of security standards and encryption protocols than compared with Tier 1 data, at	Restricted matters, business data, email, and CRM systems. Examples include financial records and medical records such as personally identifiable education	• Restricted Matters

Public Sector Data Classification	Suggested Cloud Deployment Model	Data Examples	M.C. 78, s1964 Correspondence
	agency discretion. Must have encryption to deal with restricted data.	records, personally identifiable financial information (PIFI), protected health information	
Tier 3: Confidential or above–Sensitive Data	Confidential data may require a private cloud deployment to achieve the security required for sensitive data, at agency discretion. Must have encryption.	Political documents dealing with matters of international negotiations, Technical matters of military value, major governmental projects such as proposals to adjust the nation's economy (before official publication) internal audit data, trade secrets, technical data supporting technology transfer agreements	• Confidential Matters, • Secret Matters • Top Secret Matters

SECTION 10. SECURITY

10.1 The benefit of migrating government workloads and data onto GovCloud or to public cloud is the ability to enhance overall data security. Accredited CSPs in GovCloud will meet international security standards, will be certified appropriately and will abide by all relevant Philippine laws and industry standards.

10.2 Government agencies will be expected to develop a security framework applying a risk management approach towards their own data control requirements (see **SECTION 9. DATA CLASSIFICATIONS**), and align this with internationally recognized standards and certifications, as well as Philippine industry standards. The precise baseline level of security requirements for contracted cloud services is laid out in **SECTION 11. SECURITY FRAMEWORK** below. In determining their overall risk management approach beyond this baseline, agencies may refer to the National Cybersecurity Plan 2022 for guidance. Stipulated security controls can include any one or more of the following:

10.2.1 Personnel Security
10.2.2 Physical and environmental security
10.2.3 Business continuity management and incidence response
10.2.4 Inventory and configuration management
10.2.5 Data encryption
10.2.6 Access controls, monitoring and logging
10.2.7 Network security and monitoring
10.2.8 System security and integrity

SECTION 11. SECURITY FRAMEWORK

11.1 Managing the security of contracted cloud services is a responsibility that is shared between the contracting agency and the cloud service provider, with the contracting agency responsible for selecting and implementing security controls for any workloads that it operates in the cloud, while the cloud service provider is responsible for ensuring that the services used by the contracting agency are highly secure and resilient so they are available to use on demand.

11.2 Data security of both GovCloud and the public cloud depends upon:

11.2.1 Meeting security requirements for each data classification level; and
11.2.2 Employing standardized tools and procedures for audit.

11.3 Data that can be migrated to GovCloud or the public cloud will need to meet security requirements for accreditation and be verified by internationally recognized security assurance frameworks. Accepted international security assurance controls include ISO/IEC 27001, Service

Organization Controls Report (SOC) 1 and 2, and the Payment Card Industry Data Security Standard (PCI DSS). Data will be encrypted using industry-tested and accepted standards and algorithms, such as AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits or higher), ECC (160 bits or higher), and ElGamal (1024 bits or higher).

The table below outlines the baseline (i.e. required) and <u>optional</u> (i.e. agency discretion applied) security controls that will be applied to classified government data, which accredited CSPs and GovCloud must have met to be permitted to host classified government data.

SECURITY CONTROLS	**BASELINE CERTIFICATION AND/OR PROTOCOL REQUIRED**	**DESCRIPTION**
Security Assurance Requirements	• ISO/IEC 27001 - Information Security Management • Payment Card Industry (PCI) Data Security Standard (DSS) • *<u>Optional</u>: Service Organization Control (SOC) 1 and 2* • *<u>Optional</u>: ISO/IEC 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*	These are the baseline and *<u>optional</u>* Security Assurance Requirements for Cloud Service Providers to be accredited on GovCloud. These Security Assurance Requirements ensure that Cloud Service Providers have the necessary security certifications to host government workloads.
Encryption Requirements	• AES (128 bits and higher) • TDES (minimum double-length keys) • RSA (1024 bits or higher) • ECC (160 bits or higher) • ElGamal (1024 bits or higher).	These are the baseline Encryption Requirements for Government Workloads before being deployed on an accredited GovCloud Cloud Service Provider. Note that while Cloud Service Providers can provide services with such Encryption technologies built in, these technologies can also be deployed by Government Agencies on such Workloads. These Encryption Requirements ensure that workload on any of the accredited GovCloud CSP is

		encrypted with the minimum baseline required by the Philippine Government.

11.4 In addition to the above outlined baseline and optional security controls, Government cloud service providers should provide logical security audit on data access, including logs and audit trails to ensure the prescribed security and privacy requirements are met. Government agencies should rely on logical audits and continuous security monitoring to ensure cloud services meet the agreed-upon data confidentiality and integrity, that there have been no data breaches, and that data and workloads are continuously available

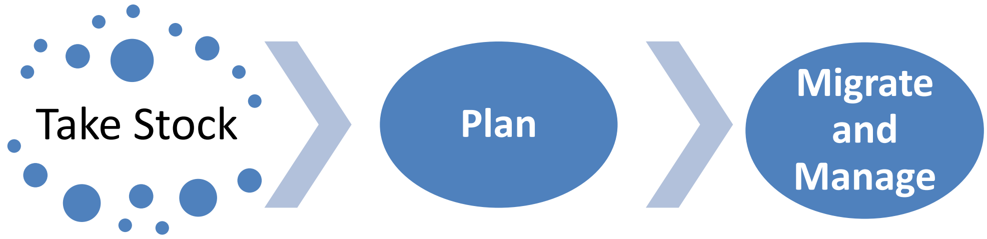
SECTION 12. DATA SOVEREIGNTY

The benefits of cloud are best realized when there is no data residency restrictions placed on data. Data residency restrictions undermine the economies of scale as well as the security benefits to be gained from shared computing infrastructure. Nevertheless, where agencies have concerns with extraterritorial access to data or where Tier 3 Confidential and above-Sensitive Data are involved, then the appropriate security standards and controls should be employed or the agency should work with DICT to consider deploying a private, on-premise cloud solution.

SECTION 13. MIGRATION POLICY

13.1 Migrating data and workloads to the cloud enhances the availability and functionality of services and improves interoperability with a wider range of other government data and workloads. Migration to cloud also enables greater automation of certain processes, increasing the availability and agility of computing resources for processes that have variable processing demands.

13.2 Migration can be seen as a three-step process:



- Define objectives
- Identify resources and value drivers
- Determine data classifications
- Map security considerations

- Define responsibilities and reporting lines
- Identify skills gaps
- Determine data sharing and permissions
- Choose suitable cloud environment
- Create roadmap

- Migrate data and test workloads
- Track, document and analyze performance against objectives
- Iterate on cloud strategy

STEP 1. Take stock

Identify how IT resources are aligned to objectives and how costs are optimized. Take stock of entity data classifications and the corresponding security considerations. Non-sensitive workloads and those that pose low security concerns should be prioritized for migration first. Government websites, public archives, development and testing environments are more readily moved to the cloud.

The value of moving workloads to the cloud is determined by the technology lifecycle and the increased functionality that cloud can bring. Moving workloads from IT resources that are near the end of their current technology lifecycle can avoid costly investments in new IT resources.

STEP 2. Plan

Create a roadmap for migrating service to the cloud, including defining responsibilities and reporting lines. Migrating workloads to the cloud can change the skills needed within the organization, for example by requiring more developers and engineers, and fewer people concerned with managing IT infrastructure. This means working with cloud providers to understand the staff skills, training and education needed in the migration and post-migration workloads.

- Identify data that can be shared and would benefit from being shared, and requirements on security and access permissions for such data.
- Identify the suitable cloud environment, such as virtualization of legacy IT, performance and functionality requirements, costs and compatibility with legacy IT.
- Determine whether replacing existing applications with new ones or to redesign service delivery architecture from the bottom-up is preferred.

Contracted cloud services should be able to integrate with existing services and should be interoperable with locally provisioned IT. They should be contracted on an aggregated basis to meet planned data and workload migration needs.

STEP 3. Migrate and Manage
Track, document and analyze progress of the plan in an iterative manner. Monitor performance and service delivery against objectives and compare costs against the migration plan.

Following migration, adequate testing of the cloud environment needs to be performed before existing solutions are decommissioned. Testing should be performed on the basis of both typical/normal usage scenarios and extraordinary utilization/demand scenarios.

Ensure that staffs are trained in the contracting and management of cloud services through service level agreements (SLAs) with cloud vendors and possess the requisite skills to manage the migrated workloads.

SECTION 14. DATA OWNERSHIP, RETRIEVAL AND INTEROPERABILITY

14.1 Data Ownership

Government institutions will retain full control and ownership over their data, with CSP identity and access controls available to restrict access to customer infrastructure and data. CSPs should provide customers with a choice as to how they store, manage, and protect their data, and not require a long-term contract or exclusivity.

14.2 Ownership

Service contracts and other SLAs related to provisioning of cloud services for Government agencies shall clearly provide that any data migrated to the cloud remains the property of the contracting Government entity, regardless of who owns, manages or operates the cloud. The contracting agency will retain rights of data access, retrieval, modification and deletion regardless of the physical location of the cloud services, including the right to approve, deny and revoke access by third parties.

14.3 Access

Access, retrieval, modification and deletion of data remain the right of the contracting Government agency and will be reflected in the relevant service contracts. The policies and processes pertaining to data access will be defined according to the needs of the contracting entity and specified in the agreement between the Government agency and the cloud provider.

14.4 Interoperability

A major benefit of cloud computing as compared to traditional IT infrastructure is that customers have the flexibility to avoid traditional vendor lock-in and CSPs should allow customers to move data on and off their cloud platforms as needed. Interoperability of all GovCloud workloads should be based on the Philippine eGovernment Interoperability Framework (PeGIF)[1] as well as international standards, such as ISO/IEC 17203:2011 Open Virtualization Format (OVF) specification.

A cloud system's components may come from different sources including public and private cloud implementations. These components should be replaceable by new or different components from different providers and continue to work, to facilitate the exchange data between systems. CSPs are required to provide interoperability,

[1] http://www.dict.gov.ph/wp-content/uploads/2016/01/ICTO_MC2014-09001_PeGIF_Part-1.pdf and http://www.dict.gov.ph/wp-content/uploads/2016/01/ICTO_MC2015-003_PeGIF_Part-2.pdf

ensuring government agencies may be able to change CSPs easily without a lengthy procurement and implementation cycle.

14.5 Open Data

Globally, governments are increasingly making their non-restricted data available for the public to discover, access and use. These open data initiatives facilitate the development of public services, fuel entrepreneurship, accelerate research and scientific discovery and create efficiencies across multiple sectors.

Government entities should endorse the open data principle and, where technically feasible and economically reasonable, make non-restricted data available to other Government agencies and the public through the cloud. In keeping with this principle and policy, Government agencies should likewise manage their data assets to promote openness and use for the public good.

As part of the Philippine Government commitment to open governance, the open data portal (data.gov.ph) facilitates the exchange of public government data with other agencies and Filipino citizens.

SECTION 15. ACCREDITATION PROCESS FOR CSPs

15.1 GovCloud Accreditation

An accreditation process for CSPs to be listed in the Philippine GovCloud will be laid out by DICT, including the baseline security assurance requirements needed before being listed on GovCloud. This is to ensure basic levels of service reliability from GovCloud CSPs, and to assure that they have secure and controlled platforms providing the necessary array of security features which government agencies can use. Agencies should ensure that they only consider vendors who have GovCloud accreditation or vendors that can meet the accreditation process as determined by them.

15.2 Baseline Security Controls

In order to provide a higher degree of assurance to agencies looking to deploy on GovCloud, DICT provides a list of baseline certifications required to be accredited on GovCloud. Agencies should look to selecting a CSP with these baseline Security Assurances which match their functional requirements.

REQUIREMENTS	BASELINE CERTIFICATION AND/OR PROTOCOL REQUIRED	DESCRIPTION
Security Assurance Requirements	• ISO/IEC 27001 - Information Security Management • Payment Card Industry (PCI) Data Security Standard (DSS) • *Optional: Service Organization Control (SOC) 1 and 2* • *Optional: ISO/IEC 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*	These are the baseline and *optional* Security Assurance Requirements for Cloud Service Providers to be accredited on GovCloud. These Security Assurance Requirements ensure that Cloud Service Providers have the necessary security certifications to host government workloads.

Further information on these Baseline Security Assurances will be provided by the DICT.

15.3 Technical and Sector-Specific Certifications

Individual sectors may also have specific certifications required. These should be considered together with the baseline certifications required, depending on the government agency's requirements.

15.4 Service Level Agreements

The provisioning of Cloud Computing should be governed by SLAs to specify and clarify performance expectations, as well as establish accountability. The SLAs should relate to provisions in the contract regarding incentives, penalties, escalation procedures, disaster recovery and business continuity and contract cancellation for the protection of the institution, in the event the service provider fails to meet the required level of performance.

Effective management of cloud services through SLAs will enable the contracting institution to manage their systems based on objectives and output requirements. To be effective, staff must be trained in the contracting and management of cloud services through SLAs, including determining and specifying the government agency's service requirements. A sample SLA is provided in Annex A.

SECTION 16. TRANSITORY PROVISION

All government agencies with existing data centers or cloud computing facilities that are to be made part of the new GovCloud infrastructure are given two (2) years to become compliant with the requirements of Sections 10 and 11 above. They are, however, encouraged to be certified after three (3) years from the issuance of this Department Circular.

SECTION 17. REPEALING CLAUSE

All other Circulars and Issuances or parts thereof that are inconsistent with this Department Circular are hereby repealed or modified accordingly.

SECTION 18. EFFECTIVITY

This Department Circular shall take effect immediately upon filing three (3) certified true copies with the Office of the National Administrative Register, University of the Philippines Law Center and publication in a newspaper of general circulation.

APPROVED.

RODOLFO A. SALALIMA
Secretary

Annex A: Sample Service Level Agreement

This Service Level Agreement ("SLA") is a policy governing the use of [Cloud Service Name] between [Service Provider Name] and its affiliates ("[abbreviation]", "us" or "we") and users of [Service Provider Name]'s services ("you"). This SLA applies separately to each account using [Cloud Service Name]. Unless otherwise provided herein, this SLA is subject to the terms of the Customer Agreement and capitalized terms will have the meaning specified in the ____________________ Agreement.

Service Commitment
[Service Provider Name] will use commercially reasonable efforts to make [Cloud Service Name] available with a Monthly Uptime Percentage (defined below) of at least 99.95%, in each case during any monthly billing cycle (the "Service Commitment"). In the event [Cloud Service Name] does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.

Definitions
"Monthly Uptime Percentage" is calculated by subtracting from 100% the percentage of minutes during the month in which [Cloud Service Name], as applicable, was in the state of "Unavailable." Monthly Uptime Percentage measurements exclude downtime resulting directly or indirectly from any Exclusion (defined below).

1) "Unavailable" and "Unavailability" mean that [Cloud Service Name] is "Unavailable" to you.
2) "Unavailable" and "Unavailability" mean:
   a) When all of your running instances on [Cloud Service Name] have no external connectivity.
   b) When all of your attached volumes on [Cloud Service Name] perform zero read write IO, with pending IO in the queue.
   c) A "Service Credit" is a dollar credit, calculated as set forth below, that we may credit back to an eligible account.

Service Commitments and Service Credits
Service Credits are calculated as a percentage of the total charges paid by you (excluding one-time payments such as upfront payments made for Reserved Instances) for [Cloud Service Name] affected for the monthly billing cycle in which Unavailability occurred in accordance with the schedule below.

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.95% but equal to or greater than 99.0%	10%
Less than 99.0%	30%

We will apply any Service Credits only against future [Cloud Service Name] payments otherwise due from you. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the Unavailability occurred. Service Credits will not entitle you to any refund or other payment from [Cloud Provider Name]. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the Customer Agreement, your sole and exclusive remedy for any unavailability, non-performance, or other failure by us to provide [Cloud Service Name] is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

Credit Request and Payment Procedures
To receive a Service Credit, you must submit a claim through our Support Center. To be eligible, the credit request must be received by us by the end of the second billing cycle after which the incident occurred and must include:

- the words “SLA Credit Request” in the subject line;
- the dates and times of each Unavailability incident that you are claiming;
- the affected [Cloud Service Name] instance IDs or the affected [Cloud Service Name] volume IDs; and
- your request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks).
- If the Monthly Uptime Percentage of such request is confirmed by us and is less than the Service Commitment, then we will issue the Service Credit to you within one billing cycle following the month in which your request is confirmed by us. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

[Cloud Service Name] SLA Exclusions
The Service Commitment does not apply to any unavailability, suspension or termination of [Cloud Service Name], or any other [Cloud Service Name] performance issues: (i) that result from a suspension of the Customer Agreement; (ii) caused by factors outside of our

reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of [Cloud Service Name]; (iii) that result from any actions or inactions of you or any third party, including failure to acknowledge a recovery volume; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); (v) that result from any maintenance as provided for pursuant to the Customer Agreement; or (vi) arising from our suspension and termination of your right to use [Cloud Service Name] in accordance with the Customer Agreement (collectively, the "[Cloud Service Name] SLA Exclusions"). If availability is impacted by factors other than those used in our Monthly Uptime Percentage calculation, then we may issue a Service Credit considering such factors at our discretion.