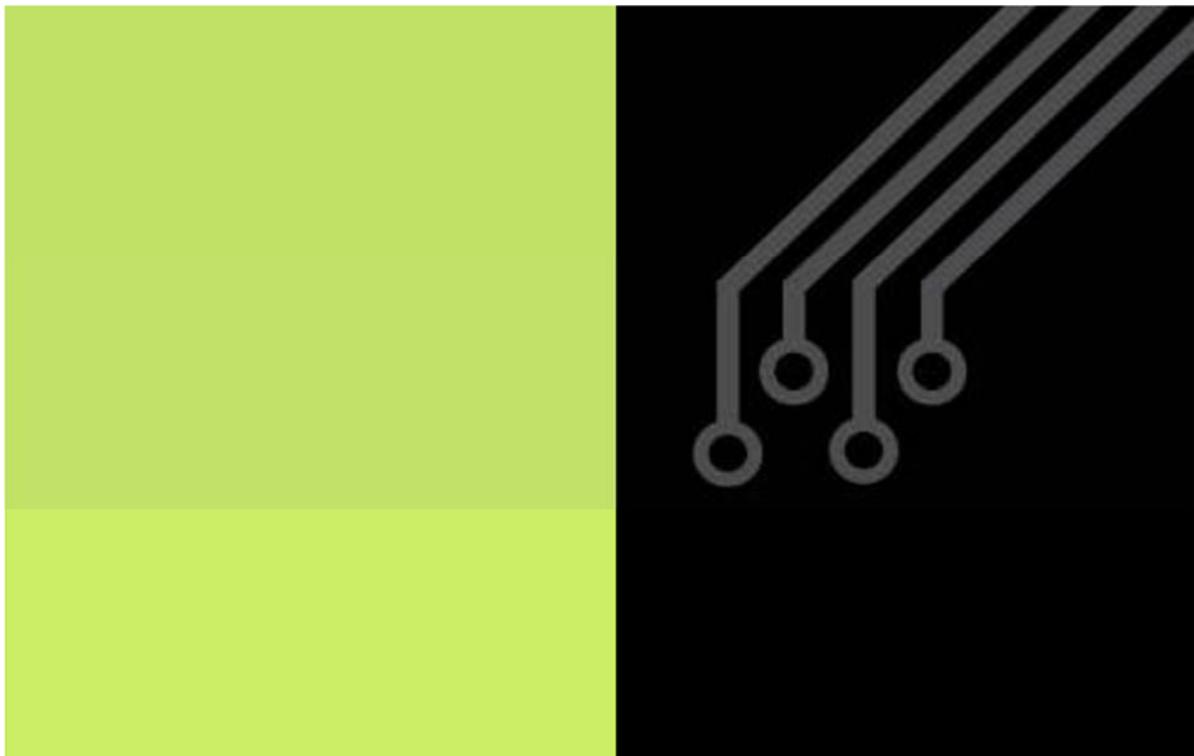# NATIONAL GUIDELINES ON CLOUD COMPUTING FOR GOVERNMENT, MINISTRIES, DEPARTMENTS AND AGENCIES

DOCUMENT DETAIL

Security Classification	Unclassified
Authority	National Information Technology Authority - Uganda
Date	October 2018
Version	CPG1

TABLE OF CONTENTS

ACCRONYMS

EGI   Electronic Government infrastructure

GoU   Government of Uganda

ICT   Information and Communications Technology

IT   Information Technology

MDA   Ministry, Department and Agency

NBI   National Backbone Infrastructure

PREAMBLE

The rate of advancement in technology has greatly transformed the way in which organizations make the best use of Information Technology (IT) to deliver services that support their business operations. For Governments, this transformation is being realized through the use of shareable infrastructure and integrated systems to efficiently deliver services. The National Information and Communications Technology (ICT) Policy (2013) further emphasizes that world over, ICT has revolutionized the way production, market access and distribution of goods and services are organized. This has led to new business models emerging on the horizon leading to fundamental changes in the way enterprises work.

In line with the above, Cloud Computing has emerged as a new model for organizations to meet their IT computing needs in an efficient, cost effective and easily scalable manner using shared infrastructure with the following attributes:

a) Users only pay for the computing resources they need;

b) Users can easily scale up or down their resources to meet their business needs;

c) Users can rely on the standardized set up (both technical and managerial) of cloud computing environments in terms of performance, data security and availability as well as resilience; and

d) The cost of the services is more cost effective as compared to the high capital and operational cost of implementing and traditional in-house IT systems.

In addition to the above, cloud computing frees up user's resource from managing complex IT infrastructure to focus on the delivery of an IT service that meets their organization or business objectives. This as well serves an enabler for innovation.

1.0 BACKGROUND

Due to the realization of the potential of ICT to enhance service delivery, the Government of Uganda (GoU) within the National Development Plan (2010/2015) classified ICT one of the key pillars to spur socio-economic development of the country. In line with this, an increasing number of Government Ministries, Departments and Agencies (MDAs) have implemented IT services for both internal and external processes based on a mixed approach for the underlying IT infrastructure using traditional IT infrastructure and/ or off-shore data hosting services. This has led to the establishment of IT infrastructure in silos with high capital and operational costs considering the rapid technological changes that require frequent investments to upgrade.

Based on the above, Cloud Computing offers the better approach for the provision of IT infrastructure at a national level. IT infrastructure resources are centralized and shared across various organizations to increase efficiency with a better value proposition on investment based on economies of scale.

In retrospect, GoU put in place the National Data Center as the 'Government Cloud' to provide centralized hosting services for Government applications and data.

Increased utilization of the Cloud will alleviate the current state of infrastructure silos, reduce risk and shift the focus to IT services as a utility. This in the long term eliminates duplication, reduces risk exposure and enhances information sharing as well as interoperability of e-government applications. At the strategic level, the Cloud provides the necessary platform for Government to provide a more interoperable hosting environment for data and systems as well as introduce common services built on shared infrastructure and economies of scale. The Government Cloud further supports the realization of the following benefits:

Domain	Benefits
Costs	• Reduced infrastructure costs

	• Reduced internal IT staff costs • Reduced operational costs such as on power and cooling
Infrastructure Management	• Improved backup/ disaster recovery • Increased information security protection and resilience • Increased asset utilization
Agility	• Purchased as a service • Increased response to business needs with near instantaneous increases or reductions in computing resources • Quicker deployment times • Provide greater choice
Innovation	• Shift focus from IT infrastructure ownership to service management • Enhanced access to improved technology • Improved productivity in application development and management

The Government Cloud will enable MDAs focus their resources on service based delivery rather than asset based delivery. The Government Cloud has been established to support the following service delivery models:

a) Infrastructure as a Service;

b) Software as a Service; and

c) Platform as a Service.

2.0 DEVELOPMENT CONTEXT

These guidelines have been developed in context with the following National Policies, Legislation and Strategies.

2.1 The National Information Technology Authority, Uganda (E-Government) Regulations, 2015

The regulations under section five (5) provide for the establishment of a National Data Centre to promote e-government based on the following:

a) Hosting services;

b) Data centre services; and

c) Disaster recovery services.

The National Data Center setup under the Electronic Government infrastructure (EGI) provides the required environment for the Government Cloud. Furthermore, the regulations under section ten (10) state that all public bodies shall use the National Data Transmission Backbone (NBI) and Electronic Government infrastructure (EGI) as the primary vehicle for all Government data, Internet and voice services.

2.2 The ICT Sector Strategic Investment Plan

The Plan identified key thematic areas as the basic fundamental clusters of influence leading to the realization of its vision. The third thematic area indicated in the plan focuses on 'ICT for service delivery.' Under objective thirteen (13) of this thematic area, the plan provides for establishment of a national data center, disaster recovery center and secure Government Cloud (U-Cloud) to ensure presence of effective and efficient e-Government services.

2.3 Strategy paper on Rationalization and Harmonization of Information Technology (IT) initiatives and services in Ministries, Departments and Agencies

The Strategy was developed to ensure full harmonization of IT operations in Government of Uganda. Under Strategy 2, the paper provides for centralized hosting services, data center services and disaster recovery services for Government applications and data. The intent is to minimize duplication and enhance inter-operability among e-Government applications.

3.0 GUIDING PRINCIPLES

The guiding principles for Cloud Computing Guidelines include following:

a) **High agility, scalability and mobility**: Computing resources are available in real time and on demand.

b) **Simplified, connected Government**: MDAs are able to share information via interoperable cloud services, supporting interagency collaboration and facilitating the development of integrated government services.

c) **Strategic ICT Delivery**: MDA ICT functions work to deliver strategic objectives and enhance service delivery, while dedicating minimal resources to the management of physical assets.

d) **Trust and Resilience**: MDA data and computing resources are secure and always available.

e) **Protection of Information**: all MDA information assets are adequately protected against cyber threats

4.0 THE CLOUD COMPUTING GUIDELINES

4.1 Goal

The goal of these guidelines is to support the usage of the Government Cloud for the provision of efficient services by Government Ministries, Departments and Agencies based on shareable infrastructure as well as achieve information assurance for Government of Uganda information assets. All Government Ministries, Departments, Agencies and Local Governments must comply.

4.2 Objectives

The objectives are:

a) To promote the use of shareable IT infrastructure for enhanced service delivery;

b) To create a more flexible, connected and agile public sector;

c) To increase value for Government on IT infrastructure investment; and

d) To provide for the protection of GoU information assets.

4.3 Guidelines

The National Cloud Computing guidelines require all Government Ministries, Departments, Agencies and Local Governments to:

a) Adhere to the use of 'Cloud First' for the design of IT enabled services;

b) Ensure that all information assets classified as OFFICIAL, SECRET and TOP SECRET are hosted in the Government Cloud;

c) Utilize the Government Cloud when procuring new ICT requirements;

d) Apply to National Information Technology Authority, Uganda for cloud services exceptions; and

e) Migrate all existing classified IT enabled services at contract expiry and/ or natural ICT refreshment points to the Government Cloud.

5.0 RISK MANAGEMENT

The concept of cloud computing has been taken up faster by private sector companies that have invested in the provision of off shore cloud services to prospective clients. The rise in the use of offshore cloud computing services raises the following risks:

a) The ownership of organizational data is uncertain since it is stored and processed on off shore third party cloud infrastructure. In most cases, cloud computing involves multi-vendors with different locations;

b) Privacy and security challenges of organizational data against cyber threats and third party access in offshore environments. The differences in law in jurisdictions creates challenges in providing appropriate legal protections; and

c) Vendor lock-in which creates challenges in transfer of organizational data in between cloud service providers.

The risks posed to Government information assets can be better managed in controlled environment in the Government Cloud. Based on the above, the Government Cloud provides a mitigation mechanism to increase assurance for GoU information assets that fall within the OFFICIAL, SECRET and TOP SECRET classification levels as defined in the National Information Security Framework (NISF) Security Classification Standard. The

classification further provides guidance on the business impact levels as noted in the table below:

Classification Level	Impact Level	Business Impact
UNCLASSIFIED	0	Trivial
UNCLASSIFIED – PERSONAL	1	Low
OFFICIAL	2	High
SECRET	3	Extreme
TOP SECRET	4	Catastrophic

The following explanatory notes describe each classification level:

a) UNCLASSIFIED: routine information and communications within the public sector. This category includes a wide range of information assets that are of low value and sensitivity to GoU.

b) UNCLASSIFIED – PERSONAL: information dealing with identifiable individuals. This category includes a wide range of information of value and sensitivity to individuals.

c) OFFICIAL: information dealing with valuable and sensitive information in control of a public body. This category includes a wide range of information relating to law enforcement, public safety, public order, and public service delivery, regulation of critical national sectors (communications, banking, utilities, etc), routine international relations as well as low level security and intelligence activities in support of public order.

d) SECRET: information that is highly sensitive that if compromised could have extremely serious consequences on GoU and/or its partners.

e) TOP SECRET: information that is enormously sensitive that if compromised could have catastrophic consequences on GoU and/or its partners.

In line with the above, all Government data within the categories of Official, Secret and Top Secret shall be stored or processed onshore in the Government Cloud. Every Ministry, Department, Agency and Local Government is required by the National Information Security Framework to classify their information assets based on business impact

assessment. The business impact of a security incident or compromise will guide the selection of the applied classification level.

5.1 Exceptions for using offshore cloud computing

The exception for Government Agencies using offshore cloud computing services such as 'hybrid on premise applications' or 'cloud based office productivity applications' shall be approved on a case by case basis by the National Information Technology Authority – Uganda using the 'ICT approval Form N7'. It is strongly recommended that the application is supported by a Business Impact Assessment as guided by the National Information Security Framework. In the Budget Execution Circular for FY2016/17 dated 29 June 2016 and Ref: BPD86/107/02 the Permanent Secretary/Secretary for Treasury (PS/ST) in Section E, 18 (ii) instructed that all Information and Communications Technology (ICT) Services must be sourced with the approval of NITA-U.

For commonly used cloud based office productivity applications, NITA-U shall offer technical assistance to undertake the risk assurance and negotiate for Government Enterprise licensing. In addition, NITA-U shall maintain an updated list on its website for accepted hybrid and/or offshore cloud based services.

6.0   GOVERNANCE

6.1 The Ministry of Information Communications Technology and National Guidance

The Ministry has the responsibility for the overall oversight of the ICT sector.

6.2 National Information Technology Authority - Uganda

NITA-U has the responsibility to:

i.   Establish and maintain the National Data Center supporting the provision of a secure and certified Government Cloud, centralized trusted shared hosting

services, national data center and disaster recovery services for all MDAs and LGs. These services shall be provided under Memorandum of Understanding covering the following at a minimum:-

   a) Service Level Agreements

   b) Clear definition of services

   c) Business Continuity

   d) Incident Management

   e) Protection of information and client applications

   f) Definition of responsibilities, especially pertaining to systems management

ii. Provide ICT strategic planning and risk management support to MDAs and LGs

iii. Approve exceptions for Government MDAs and LGs for use of cloud services using the N7 Form

iv. Publish and maintain on its website-accepted cloud based services to guide the selection of hybrid cloud computing based applications.

6.3 Government Ministries, Departments, Agencies and Local Governments

Following the publication of this guideline, each MDA has the responsibility to:

   i) Classify all information assets as guided by the Technical Risk Assessment and Security Classification standards of the National Information Security Framework and submit the same to NITA-U for information assurance

   ii) Re-evaluate its technology sourcing strategy to include use of the Government Cloud

   iii) Submit all ICT service requirements for assurance and approval to NITA-U using the N7 form

   iv) Submit requests for hybrid or cloud services exception approval to NITA-U

   v) Develop migration plans to transfer existing IT services based on their risk assessment and natural IT refresh points to the Government Cloud in order to improve IT flexibility, responsiveness and minimize cost.

7.0 MONITORING AND EVALUATION

Realization of the outputs of these guidelines will require consistent monitoring and evaluation of the outcome indicators. Two major monitoring and evaluation activities will be carried out periodically. These are impact assessment and periodic performance assessments and review as noted below:

a) Impact assessment and evaluation will be carried out after five years of implementation to assess its contribution to the economy and inform future ICT strategic planning processes;

b) Implementation of monitoring will be carried out on an Annual basis to establish whether the implementation is on schedule and assist in correcting deviations (if any) and bring the implementation back on course.