POLICY FOR THE ADOPTION OF CLOUD SERVICES BY GOVERNMENT ORGANIZATIONS IN SRI LANKA

DRAFT V 1.14

2 July 2024

Ministry of Technology

VERSION HISTORY

Version	Date	Comment
1.0	21.03.2022	Initial Draft
1.1	24.03.2022	First Review – Director, Policy – ICTA
1.2	29.03.2022	First Review – Director, Infrastructure Services – ICTA
1.3	30.03.2022	First Review – Director/Architect – ICTA
1.4	01.04.2022	Second Review – Director, Infrastructure Services – ICTA
1.5	04.04.2022	Third Review – Director, Infrastructure Services – ICTA
1.6	19.04.2022	Fourth Review – Director, Infrastructure Services – ICTA
1.7	26.05.2022	Review by the Information Security Team – ICTA
1.8	07.11.2023	Revisit by the Data Infrastructure and Data Services Thematic Working Group headed by the World Bank
1.9	23.11.2023	Review 1 – CXOs/Directors – ICTA
1.10	31.01.2024	Review with Senior Manager, Network and Infrastructure Solutions – ICTA
1.11	06.02.2024	Review 2 – CXOs/Directors – ICTA
1.12	12.02.2024	Review 3 – CXOs/Directors – ICTA
1.13	21.03.2024	Review by Acting Digital Economy Officer/Acting CDGO – ICTA
1.14	30.05.2024	Review by Ministry appointed Review Committee – Round I

LIST OF ABBREVIATIONS

CSP	Cloud Service Provider
FoC	Free of Charge
GoSL	Government of Sri Lanka
IaaS	Infrastructure as a Service
MoU	Memorandum of Understanding
MTTR	Mean Time to Repair
NDX	National Data Exchange
NSDI	National Spatial Data Infrastructure
PaaS	Platform as a Service
PT	Penetration Testing
RoI	Return on Investment
SaaS	Software as a Service
TAM	Technical Account Manager
VA	Vulnerability Assessment
VMs	Virtual Machines

LIST OF TABLES

LIST OF FIGURES

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Background

The Government of Sri Lanka has recognized the importance of Digital Transformation in building an advanced, prosperous, and inclusive nation leading to an improved digital economy. This directly follows the adaptation of emerging technologies, in order to become more efficient and productive in information and service delivery. Data storage and connectivity in the public sector become decisive factors in ensuring that government services and information are available in a more agile, faster, cheaper, economical and secure manner. In view of that, the Government of Sri Lanka recognizes moving towards Cloud Infrastructure and Solution Services as a key enabler in making a shift from its traditional data storage and computing framework towards a more robust, effective, economical and secure landscape.

1.2 Need

The shift from the traditional data storage mechanisms towards Cloud Computing Solutions requires attention on formulating appropriate guidelines to ensure security and data protection, whilst enabling secure data flows. This demands a 'Cloud Adoption Policy/Guideline for Government' to provide the direction for government organizations to obtain the benefits of Cloud Computing and Storage Solutions in a manner that would promote efficiency, accuracy, interoperability, and security of data handled by them.

1.3 Purpose and Scope

The policy/guideline aims to prioritize the procurement of cloud based ICTs and promote widespread adoption of cloud services by Government organizations[1] as part of their IT investment decision-making process.

This will apply to infrastructure, hardware, software, information security, licensing, storage and provision of data, as well as services like security, development, virtualization, databases or any kind of technology where a cloud solution is equivalent to other forms of technological solutions.

1.4 Rationale

As per the definition of the U.S. National Institute of Standards and Technology (NIST);

[1] All Government organizations that comply with the Right to Information (RTI) process.

"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 essential characteristics, three service models, and four deployment models".

The policy is devised on the basis of the following key aspects.

a. Government organizations should be encouraged towards the optimal usage of cloud services to achieve higher degree of efficiency and productivity.

b. Emerging technology developments should be explored in the achievement of the government's digital transformation efforts and ensure the availability of required resources for such achievement.

c. Cost of total solutions i.e. purchasing, setting up, running and maintaining information services, in the public sector should be minimized.

d. Government organizations should be empowered to respond to citizens and businesses in a more effective, efficient and productive manner.

e. Resilience of digital government services should be improved thorough a more developed service continuity and disaster recovery framework.

The policy aims to drive greater acceptance of cloud services in the public sector by adopting a 'cloud-first' approach to promote better infrastructural investments and an efficient IT deployment in the public sector.

1.5 Applicability

a. The policy shall apply to all government organizations and officers, including statutory bodies, as defined in the applicable legislation to Government service.

.

2 THE NEED FOR A 'CLOUD FIRST' APPROACH

The Government of Sri Lanka strongly advocates for a 'Cloud First' strategy when government organizations require hosting services. Accordingly, all government organizations shall adopt cloud service as the preferred strategy for new ICT service deployment and also when transforming the existing services to digital applications, except if it can be shown that an alternative ICT deployment strategy;

- Meets special requirements of the government organization or
- More cost effective from the perspective of Total Cost of Ownership (TCO)[2] or
- Demonstrates the same level of security assurance that a cloud solution offers; or
- The particular cloud service or technology required by the government organization, is not available in Government Cloud.

Alternative solutions, such as on-premises, can only be explored as a last resort if a cloud-based solution is impractical. This is the recommended approach for the entire public sector unless organizational-specific circumstances stand as a hindrance.

[2] Refer Annex 1 – Total Cost of Ownership

3 PRINCIPLES TO FOLLOW

The selection of a suitable cloud service provider (CSP) constitutes a fundamental decision in a successful cloud migration journey. Adherence to a defined set of principles, would drive organizations towards informed decisions throughout the migration journey, maximizing the Return on Investment (RoI).

The policy recommends Government organizations to prioritize the eight (8) principles outlined in this section, when choosing a CSP. These principles act as essential safeguards to ensure that the most suitable CSP, who could deliver optimal outcomes, is chosen.

Figure 1: Policy Principles

4 POLICY STATEMENTS

Policy Principle 1 – Security

Objective 1 – Ensure the secure deployment of Government data and services to the cloud infrastructure, safeguarding sensitive information and mitigating potential risks, thereby fostering trust, resilience, and continuity in digital governance.

Policy Statement 1.1

Government organizations must classify data based on sensitivity, in alignment with Information Classification Policy for Government Organizations, complying with standardization guidelines of NIST SP 800-53 to ensure only authorized personnel can access specific data types.

Data deemed highly sensitive and classified as 'Secret' – encompassing cabinet memoranda, information on defense, public security and foreign affairs – must be stored and processed exclusively within national borders. Transferring such data to foreign-based systems connected to the public internet would pose a significant risk to national security interests.

Policy Statement 1.2

The decision on data residency lies with the Government organizations. The CSP must comply with Sri Lankan data protection laws and regulations in consultation of the respective Government organizations.

Policy Statement 1.3

Data at rest and in transit should be encrypted using industry-standard algorithms. The Government organization to retain control over encryption keys and manage them securely.

Policy Statement 1.4

Existence of a robust incident response plan, which aligns with standardization guidelines of NIST SP 800-53; to identify, contain, and recover from data security breaches. Timely reporting of incidents to relevant authorities is mandatory.

Policy Statement 1.5

Regular security audits of cloud environments to be conducted to ensure adherence to security standards. The CSP must prove relevant security certifications such as ISO 27001.

Policy Principle 2 – Data Sovereignty

Objective 2 – Ensure sovereignty over data and cloud infrastructure, thereby safeguarding sensitive information, protecting national security interests, and promoting trust in cloud services.

Policy Statement 2.1

Ensure adherence to relevant laws, regulations, and international standards governing data protection, privacy, and cyber security. Government organizations must conduct thorough assessments of CSP compliance on certifications, security protocols, and contractual commitments to safeguard national sovereignty and mitigate legal risks.

Policy Statement 2.2

Government organizations (i.e. Public Authorities) should process personal data in Sri Lanka to the extent required by the Personal Data Protection Act, No. 9 of 2022.

However, public authority has the ability to consult the Data Protection Authority and classify the categories of personal data which may be hosted outside Sri Lanka.

Policy Principle 3 – Cost Optimization

Objective 3 – Strategically implement Government IT infrastructure and services to the cloud with a primary focus on cost optimization, aiming to reduce operational expenses, enhance resource efficiency, and maximize the RoI whilst ensuring continued delivery of high quality and secure digital services to citizens and stakeholders across Sri Lanka.

Policy Statement 3.1

Conduct a thorough cost-benefit analysis considering capital costs, deployment costs, maintenance costs, management costs, subscription fees, data transfer costs, exit costs and potential cost savings from resource optimization.

Policy Statement 3.2

All Government organizations should regularly assess the cloud infrastructure to identify underutilized resources, unused services, and areas for optimization in a manner which encourages the adoption of auto-scaling and right-sizing practices, to ensure that the resources are provisioned appropriately to meet demand while avoiding unnecessary costs.

Policy Principle 4 – Sustainability

Objective 4 – Leverage cloud technology to achieve optimal resource utilization and minimize energy consumption, thereby achieving sustainability.

Policy Statement 4.1

Adopt a cloud-first policy, prioritizing the use of cloud-based services for all new IT projects and gradually migrate existing services to the cloud where feasible.

Policy Statement 4.2

Leverage the efficiencies and scalability of cloud technology to reduce the energy consumption of data centers and improve the overall sustainability of IT infrastructure.

Policy Statement 4.3

Ensure that cloud service providers adhere to strict sustainability and energy efficiency standards, thereby aligning IT operations with broader environmental objectives and enhancing the innovation and accessibility of public service delivery.

Policy Statement 4.4

The Government shall prioritize the procurement and deployment of energy-efficient IT equipment and services. This includes mandating the use of devices and infrastructure that meet recognized environmental standards and certifications. Furthermore, the Government will implement rigorous lifecycle management practices, including responsible e-waste recycling programs, to ensure the minimal environmental impact of IT operations. These measures will collectively reduce the ecological footprint of Government IT operations while supporting sustainable development goals.

Policy Principle 5 – Transparency and Accountability

Objective 5 – Enhance transparency and accountability in the procurement and management of public cloud resources, thereby fostering increased public trust.

Policy Statement 5.1

It is imperative to ensure transparent procedures in the procurement and management of cloud resources. The critical aspect of cost optimization should be given utmost importance when acquiring cloud resources. This involves conducting a thorough evaluation of prices offered by multiple vendors, comparing them against the same solution, and considering their respective SLA conditions.

Policy Principle 6 – Operational Efficiency

Objective 6 – Strategic adoption of cloud technologies and best practices to optimize resource utilization, reliability and agility (ability of an organization to quickly scale resources up or down, adapt to changing workloads, and respond to market demands) across Government organizations.

Policy Statement 6.1

All government organizations in Sri Lanka should adopt a 'Cloud-First' approach for IT infrastructure and application deployment.

Policy Statement 6.2

Develop and implement a comprehensive cloud deployment strategy for transitioning new and existing IT systems and applications to a secure and scalable cloud infrastructure.

Policy Statement 6.3

Establish open and standardized protocols, open APIs, and open data formats to facilitate data exchange and interoperability, enabling efficient collaboration and service delivery.

Policy Statement 6.4

Government organizations should invest in training programs for public sector employees on cloud technologies, security best practices, and cloud-based tools. This empowers staff to leverage the full potential of the cloud for improved efficiency.

Policy Statement 6.5

Implement robust monitoring and optimization mechanisms to continuously assess the performance, security, and cost-efficiency of cloud-based systems and services. Regular audits and reviews shall be conducted to identify opportunities for improvement and ensure adherence to established policies and standards.

Policy Principle 7 – Scalability

Objective 7 – Leverage cloud computing to scale IT resources to meet fluctuating demands, ensuring optimal service availability.

Policy Statement 7.1

The cloud strategy of the Government organizations should consider future growth and evolving needs, with a focus on flexibility and scalability of CSP infrastructure to adapt to the changing demands and technological advancements.

Policy Statement 7.2

Government organizations should ensure that the selected cloud solution facilitates flexibility to scale resources both vertically and horizontally according to demand in order to optimize resource utilization, minimize costs, and maintain performance during peak periods.

Policy Principle 8 – Disaster Recovery and Operational Continuity

Objective 8 – Guarantee uninterrupted delivery of Government services, by leveraging cloud resources and ensure that the Cloud Service Provider (CSP) understands and delivers the requirements according to the demands of the Government client.

Policy Statement 8.1

All Government organizations implementing solutions in the cloud must develop and adhere to a comprehensive Disaster Recovery (DR) plan, in alignment with the best practices and the specific needs of each organization's critical applications and data.

Policy Statement 8.2

All Government organizations must evaluate and select a CSP that offers robust disaster recovery solutions, focusing on regular back-ups and automated failover mechanisms to ensure minimal downtime in case of disruptions.

Policy Statement 8.3

All Government organizations should ensure that the CSP's cloud DR plan is integrated with the operational continuity of each organization, in order to guarantee a coordinated approach that minimizes disruption to core services and public access to information.

Policy Statement 8.4

Government organizations should implement regular data back-ups to the cloud, with a focus on critical data and applications.

5 A COMPARISON OF CLOUD MIGRATION APPROACHES

The choice of a cloud service provider depends on the specific needs and priorities of each government organization. Factors to consider include security requirements, compliance mandates, performance demands, budget constraints, and existing IT infrastructure. Carefully evaluating these factors and aligning them with the strengths of each cloud provider will lead to a well-informed decision that supports the organization's mission and objectives.

Government organizations are encouraged to select either of the following options that best aligns with their unique needs and the policy principles.

1. Government Cloud (GOVERNMENT CLOUD)
2. Commercial Cloud in Sri Lanka (Local CSP)
3. Off-shore Cloud (International CSP)

This table offers a comparative analysis of different CSP options available to Government organizations, against the policy principles discussed above. It aims to facilitate the selection of the most appropriate CSP based on the recognized policy principles.

Principle	GOVERNMENT CLOUD	Local Cloud	International cloud
Data Security	Provides complete security protection for the infrastructure. In addition, client will be responsible for applying security precautions for the applications hosted in GOVERNMENT CLOUD.	Alignment with these principles may vary significantly between different CSPs.	Alignment with these principles may vary significantly between different CSPs.
Data Residency	Data sovereignty aspects are fully guaranteed in alignment with Sri Lankan legal and regulatory landscape.	In order to ensure optimal alignment with the policy principles, government organizations are	In order to ensure optimal alignment with the policy principles, government
Cost Optimization	Currently, offered on Free of Charge (FoC) basis. Planning to implement Pay-as-you-go model in the next version.		

Principle	GOVERNMENT CLOUD	Local Cloud	International cloud
Sustainability	This project is owned by GoSL and currently operated by ICTA thus, sustainability is guaranteed.	advised to **caref**ully evaluate and select the CSP that best serves the same.	organizations are advised to carefully evaluate and select the CSP that best serves the same.
Transparency and Accountability	This project is owned by GoSL and currently operated by ICTA thus, transparency and accountability are guaranteed.		
Operational Efficiency	Application or data can be accessed from anywhere supported with LGN or public internet connectivity.		
Scalability	Flexibility exists to upscale/ downscale resources based on the client request.		
Disaster Recovery and Business Continuity	Strong contract with principle service providers including local support and delegated Technical Account Manager (TAM). In addition, certified GOVERNMENT CLOUD technical support team is involved in day-today operations through the Network Operations Centre (NoC).		

Table 1: Comparison of Different Cloud Adoption Options

6 CLOUD IMPLEMENTATION PROCESS

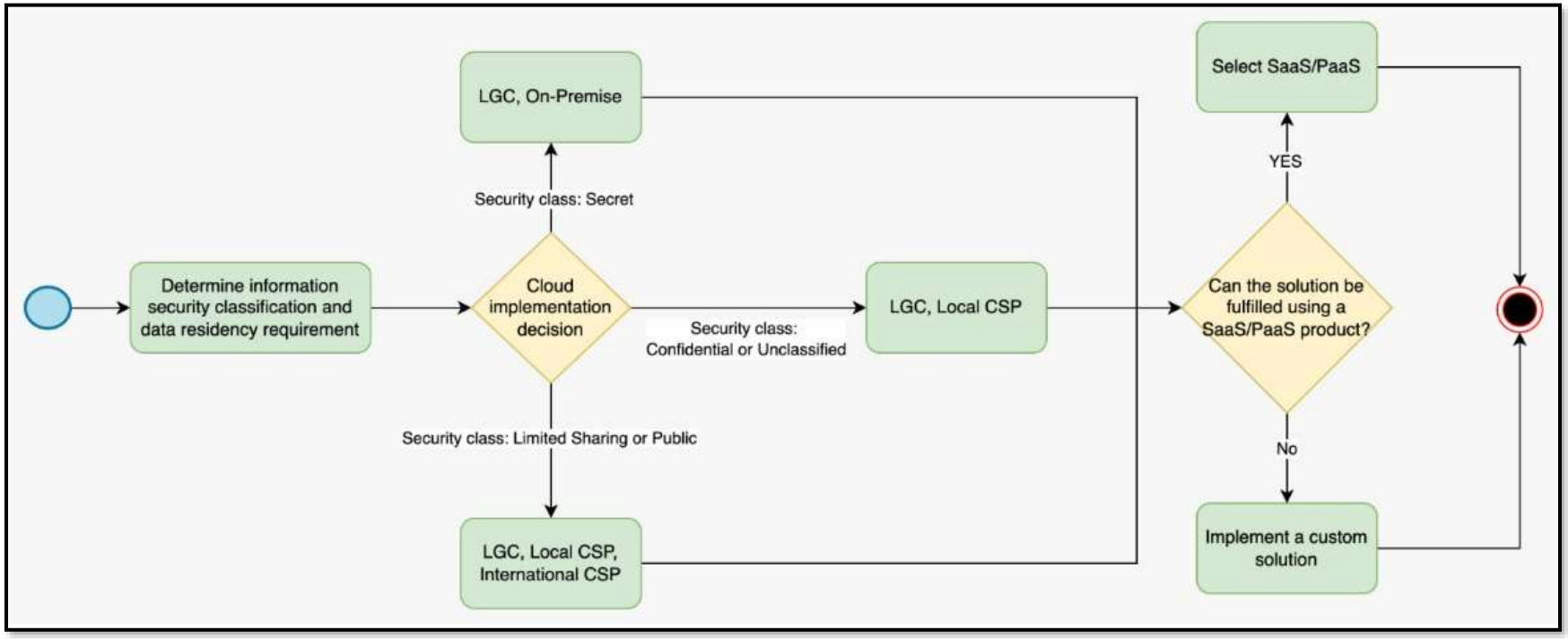

Figure 2 : Cloud Implementation Process

6.1 Deciding the type of the Cloud: Local (on-shore) or International (off-shore) Cloud

a. Determine the information security classification of the data assets, in alignment of the Information Classification Framework for GoSL, is the very first decision-making, setting the stage for subsequent decisions.

b. Based on the data classification, Government organizations can determine the type of CSP i.e. an on-shore Local CSP or an off-shore International CSP.

- 'Secret' → Only in the Government Cloud
- 'Confidential/Unclassified' → Government Cloud or a local CSP
- 'Limited Sharing or Public' → Government Cloud or local/international CSP

c. Following the selection of the CSP, the next step is to determine the nature of the cloud solution, in consideration of the following.

- If the implementation can be accommodated via a SaaS or PaaS model or;
- If SaaS or PaaS do not fully meet the requirement, opt for a customized solution.

d. This allows seamless migration of existing on-premises solutions to the cloud or implementing new solutions in the cloud, preserving their functionality while leveraging the benefits of cloud infrastructure

6.2 Deciding the components to implement

When deciding which components to implement, it is advisable to carry-out a pre-migration assessment[3] of the systems, platforms, solutions and applications that are used by the organization and decide which are to be retired, retained and implemented/migrated in the cloud infrastructure.

Type	Definition
Retire	Applications, systems, platforms or solutions which are of **no value to the organization and hardly used** by the organization.
Retain	Applications, systems, platforms or solutions which are **not cloud ready** thus, organization can retain them leaving as on-premises solutions.
Migrate	Applications, systems, platforms or solutions that the organization **decides to be moved** to a cloud environment.

Table 2 : Categorization of Migration Components

[3] Refer Annex 4 : Cloud Adoption Lifecycle

6.3 Migration Options

6.3.1 On-premises to Cloud Migration

Migration of on-premises solutions to a cloud environment. Following the comprehensive pre-migration assessment, government organizations can formulate a strategic cloud migration roadmap. This roadmap should prioritize the transfer of applications, systems, platforms, or solutions with minimal operational disruption, gradually ascending to ones with higher impact. This ensures minimal disruption to the ongoing workflows and fosters a smooth transition to the cloud environment.

6.3.2 Cloud to Cloud Migration

Migration of applications already hosted in a cloud platform to a different cloud platform. Exit or switching costs from one cloud to the other must be carefully assessed, and the decision to migrate should have sound reasoning in terms of cost and operational efficiencies, and should be made in adherence to the aspects stipulated in this policy.

6.3.3 On-premises to the Cloud Platform facilitated by the same vendor

Government organizations upon performing the pre-migration assessment can opt to migrating existing on-premises solutions to its cloud version provided by the same vendor. If the existing on-premises infrastructure are dedicated purpose-built infrastructure for this solution which is to be migrated, the assessment should ensure that such infrastructure have effectively reached or exceeded its useful lifespan, and this decision is in adherence to the aspects stipulated in this policy.

7 DATA OWNERSHIP, RETRIEVAL AND INTEROPERABILITY

7.1 Data Ownership

Government organizations must have the full control and ownership over their data, with proper measures to restrict access to customer infrastructure and data. CSP should provide a choice as to how they store, manage, and protect their data, and not require a long-term contract or exclusivity.

7.2 Retrieval and Interoperability

Government organizations should be able to utilize common ICT infrastructure and facilities such as National Data Exchange (NDX), National Spatial Data Infrastructure (NSDI), Country Portal, Mobile Portal, GovSMS, Lanka Government Payment Service (to process electronic payments) and Government Information Centre (GIC, for citizen services for providing service related information to public) via interoperable cloud services, supporting collaboration and integrated government services.

8 SERVICE LEVEL AGREEMENTS (SLAs)

a. The provisioning of cloud solutions by CSPs to government organizations shall be governed by SLAs to specify and clarify performance expectations and establish accountability.

b. The SLAs should relate to the provisions in the contract pertaining to penalties, escalation procedures, disaster recovery, business continuity, and contract cancellation for the protection of the government organization in the event if the CSP fails to meet the required level of performance, reliability and security.

c. Government organizations should closely monitor the CSP's compliance with key SLA guidelines on the following aspects, among others;

   - Software and underlying infrastructure management
   - Availability and timeliness of services
   - Confidentiality and integrity of data
   - Change control
   - Compliance with security standards
   - Compliance with data protection including backups, retention periods, rights of the data subject and encryption controls; access management and data control permissions
   - Business continuity including disaster recovery and contingency plans
   - Right to change the CSP
   - Help desk support
   - Response time and resolution time

d. The roles and responsibilities of the government organizations, CSPs, and any other parties involved such as carriers etc. should be clearly explained and stated in the SLAs.

9 DISCONTINUATION OF CLOUD SERVICES

In the event of terminating a cloud service provider (CSP) agreement, the policy recommends that Government organizations give due consideration to the following aspects

a. Compliance to the agreed timeframe for termination communication.
b. Evaluation of termination and transition costs.
c. Data Transfer
d. Data security during the termination process
e. Dispute resolution mechanism during the termination process.

10 ADMINISTRATION AND ACCESS LEVELS

a. The existence of a valid agreement with a special focus on the confidentiality of data

b. Access rights granted to third party service providers to access the cloud should be supported with a duly approved access authorization form.

c. Subsequent access rights granted, at different time intervals depending on organizational requirements, should get reflected in the same access authorization form.

11 GENERAL GUIDELINES

11.1 Policy Implementation Responsibility

11.1.1 Government Organizations

a. All government organizations involved in procuring cloud based services, applications or platform hosting services for the government organizations must adhere to this policy.

b. The CDIO of every government organization is responsible for ensuring the application and adherence to this policy within the organization.

c. Government organizations should take all efforts to minimize the usage and expansion of on-premises data centers, IT storage or processing infrastructure. Instead efforts should be taken to deploy cloud services as appropriate.

d. Appoint a dedicated cloud administration and support team, under the supervision of the CDIO, in order to address organizational transformation and subsequent operational efficacy.

e. Adhere to the guidelines, instructions for the use of cloud services prepared by the Ministry of Technology, and ensure that the staff apply these guidelines and instructions accordingly.

f. The government organizations shall not sign an agreement with a third party CSP prior to the completion and passing of all the mandatory controls specified in the CSP Assessment Questionnaire[4].

11.1.2 Cloud Service Provider

a. It is the responsibility of the CSP to protect its cloud system and maintain confidentiality, integrity and availability of its data.

b. Data shall not be stored, shared, processed, or modified in any manner which threatens its integrity.

[4] Refer Annex 5 : CSP Assessment Questionnaire

c. CSP should not have access to monitor their customers' data and content, thus strict adherence should be maintained to the required level of confidentiality by the government organizations.

d. CSP should be able to provide necessary support to perform periodic audits or investigations as and when required by the government organizations and any legitimate government party.

e. The failure to satisfy any of the responsibilities on the part of the CSP shall constitute a breach of the contract.

f. Identification of such a breach would necessitate the government organizations to terminate the contract with the CSP, subject to the stipulated timelines in the service contract.

g. It is the responsibility of the CSP to notify the government organization within 24 hours of a potential or actual breach or incident that may affect and threaten the organization's information hosted in the cloud.

h. CSP must provide adequate investigative support to the government organizations.

i. CSP should retain the investigation reports related to any security investigation for a period of 2 years upon the completion of the investigation progress.

j. CSP must support e-discovery and legal holds to meet the needs of investigations and judicial requests.