Cloud Services Policy

Reference:	GMICT P 0124	Publication:	13 September 2024
Version:	1.0	Effective:	13 September 2024

Purpose

To enable the utilisation of cloud services provided by Government through the Agent within the Public Administration and guide in the adoption of any needed alternative cloud services in order to safeguard Government data.

Scope

This policy deals with Government's approach to, and the utilisation of, cloud services within the Public Administration.

Definitions

Underlined terms are defined in the **Vocabulary** (GMICT X 0003).

Cloud First Strategy

Rationale

Such strategy refers to a model where cloud services are selected by an organisation the primary means to process its data. It is the benefits realised through the utilisation of cloud service, relative to traditional digitalisation methods that is of intrinsic value. Such utilisation is widely seen as a very significant means of strengthening digitalisation, improving productivity and bringing about cost savings. The flexibility, scalability and innovation offered by cloud services, including in computing capacity and storage enable more rapid developments of public services in line with technological evolvements such as those in AI.

1. A Public Administration organisation shall give **primary preference to the utilisation of Cloud services,** unless specific considerations arising from other goals require use of alternative technologies.
2. A Public Administration organisation shall select the **cloud service delivery model** that best suits its business. However, the selection shall take into account the following (numerical) order of preference[1]:

(i) Software as a Service (SaaS)

(ii) Platform as a Service (PaaS)

(iii) Infrastructure as a Service (IaaS).

Agent-provided Government Cloud Services First

Rationale

Such approach aims to enable centralisation in the use of such services and thus facilitate interoperability and economies of scale in information management within the Public Administration.

3. A Public Administration organisation **shall give primary preference** to the use of **Cloud Services provided by the Government through the Agent.**

Cases where cloud services provided by the Government through the Agent are to be selected include solutions:

a. storing, processing, transmitting or sharing **classified** information

b. **for enterprise ICT and back-office** functions

c. **in bespoke development**

d. **hosted on the Agent's infrastructure**

The selection of any cloud service that is not provided by the Government through the Agent shall need to be justified in writing by the system owner.

[1] *(The definitions being adopted for the three models referred to below are those proposed by the National Institute of Standards and Technology (NIST) Definition of Cloud Computing)*

4. If a Public Administration organisation decides that the cloud services provided by the Government, through the Agent are not the appropriate solutions for its needs, **alternative services** may be used. In such circumstances, a **contractual agreement** between the Public Administration organisation and the service provider, should be in place.

Considerations of the contractual agreement include:

- Architecture
- Technology
- Interoperability
- Vendor lock-in
- Exit strategy
- Security standards
- Assurance of confidentiality, integrity and availability of data
- Data location and retrieval
- Business Continuity and Disaster Recovery procedures
- Staffing and skill requirements
- Performance of cloud service
- Applicable service level agreements
- Value for money
- Commercial and pricing models
- Legal terms and conditions
- Legal jurisdiction for the resolution of any legal issues
- Reputation of service provider

5. If a Public Administration organisation decides that neither the cloud services provided by the Government through the Agent nor contracted services are appropriate for its needs, **free non-enterprise cloud services** may be adopted. Great care must be taken when storing, processing, transmitting or sharing information on a **free non-enterprise** cloud service in a **Government** context since it may not have the resilience and security of a larger-scale enterprise product.

A number of issues may be encountered that would be out of the Government's and the user's control and which need to be taken into account. These include, but are not necessarily limited to:

- whether the data is only being used for the intended purpose
- the number of copies that will exist on mirror servers, backups, etc.
- who will have access to the data beyond the immediate intended users
- the actual location of the data
- legal jurisdiction and therefore applicable laws and other regulations
- terms of use of these services, e.g. data retention policy
- ease of securely interfacing or integrating with Solutions on the Agent's infrastructure

Selection and procurement

Rationale

The following aim to further minimise risks of compromise in any way of Government data, particularly at the selection and procurement stages whilst keeping in view of the context in which cloud services are to be utilised.

6. A Public Administration organisation shall select the **cloud deployment model** that best suits its business. The **selection** shall be based upon **consideration and full evaluation** in **the sequence** as indicated in the Section "*Agent-provided Government Cloud Services First*" of this Policy.
7. A Public Administration organisation making use of the cloud services provided by the Government through the Agent may mandate their use in any invitation to tender (ITT) or request for procurement (RFP) as well as in the contractual agreements drawn up with their Solution Providers.
8. The **procurement, deployment and utilisation of cloud services** shall be treated in the same manner as any other procurement or change of an ICT solution.
9. As a rule, Cloud services utilised shall **be those provided within the EU/EEA** to minimise regulatory derivative risks.

Security, data protection and business continuity

Rationale

Essentially, Government information placed on any public cloud service shall need to be protected accordingly. Security controls expected for any cloud service delivery model procured as well as the corresponding roles responsible for their implementation is vested are also highlighted accordingly.

10. Reference shall be made to the *GMICT P0016 Information Security Policy* for any security-related content.
11. For procurement of **any** cloud service delivery model, the respective responsibility for implementation of specific security controls shall be vested in the roles as indicated in Appendix 1.
12. The processing of data on a public cloud service shall be based upon Risk based assessments and decisions that take into account information security, data protection and business continuity.

In the process, reference shall be made, but shall not be limited to:

- The *GMICT P 0016 Information Security Policy*, especially, but not limited to, the Security Marking of Data
- The *General Data Protection Regulation, (EU) 2016/6791* and the *Data Protection Act (CAP 586)* for personal data.

Appendix 1: Roles and Responsibilities for security controls for **any** cloud service delivery model procured.

Asset	Security Controls	*Cloud Service Delivery Model* and corresponding role(s) responsible for implementing the security controls		
		IaaS	*PaaS*	*SaaS*
Physical Hosting Environment	(i) Restrict Data Centre physical access to authorized individuals only. (ii) Minimise the effect of any physical disaster on Data Centre. (iii) Monitor fire, air conditioning and any other Data Centre equipment or activity. (iv) Protect all physical network components.	**Cloud Service Provider**	**Cloud Service Provider**	**Cloud Service Provider**
Operating System (OS)	(i) Update guest OSs. (ii) Apply any OS updates including security patches. (iii) Harden the OS.	**Customer**	**Cloud Service Provider**	**Cloud Service Provider**
Network	(i) Protect against network security threats such as DDoS. (ii) Implement controls such as Intrusion Prevention Security (IPS), Intrusion Detection Security (IDS), Firewalls, Web Application Firewalls (WAF) (iii) Implement network access measures. (iv) Monitor network availability.	**Customer**	**Shared**	**Cloud Service Provider**
Application	(i) Apply application hardening. (ii) Apply patch management. In IaaS, the customer shall ensure that the guest OS and applications residing on an Information System are updated.	**Customer**	**Shared**, where customer has control over the deployed applications	**Cloud Service Provider**

Asset	Security Controls	*Cloud Service Delivery Model* and corresponding role(s) responsible for implementing the security controls		
		IaaS	***PaaS***	***SaaS***
Identity & Directory Infrastructure[2]	(i) Enable Multi-factor Authentication (MFA) and ensure that it is in operation. (ii) Federate User Identities. (iii) Implement Logical Access Controls.	**Customer**	**Shared**, where the service provider shall ensure that the MFA is in operation, whilst the customer shall enable the service to users	**Shared**, where the service provider shall ensure that the MFA is in operation, whilst the customer shall enable the service to users
Information & Data	(i) Apply the appropriate encryption method to provide reasonable assurance that data handling between the customer and the host service provider is secure	**Customer**	**Customer**	**Customer**

[2] For access control to user services and resources

Deviations from GMICT Policy

Instances where it may not be technically possible or cost-effective to comply with a particular GMICT Policy requirement shall be reported as risks to be assessed.

Breaches of GMICT Policy shall be brought to the attention of the respective CIO office in order to determine appropriate corrective action and potential control improvements involving relevant stakeholders, as appropriate.

Issuing Authority

This document has been issued by the **Principal Permanent Secretary**.

Contact Information

Government ICT Policies may be found at **http://ictpolicies.gov.mt**.

Any suggestions, queries or requests for clarification regarding Government ICT Policies may be forwarded to **ictpolicies@gov.mt**.