Centralised Digital Enabling Services Policy

Reference:	GMICT P 0121	Publication:	10 June 2020
Version:	4.0	Effective:	10 June 2020

Purpose

To encourage the use of centralised digital enabling services within the Public Administration and guide the adoption of alternative services in order to safeguard Government data.

Scope and Applicability

This policy deals with the centralised digital enabling services made available to the Public Administration through the Agent.

Definitions

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

General

1. **Preference** shall be given to the centralised digital enabling services provided by the Government through the Agent. These include the Agent's:
    - **Cloud Services** (including the Hybrid Cloud Platform and any other cloud services provided or brokered through the Agent) especially for storing, processing, transmitting or sharing **classified** information
    - **Electronic Payment Service** (Government Payment Gateway)
    - **Notifications Service**
    - **Video Streaming Service** (Microsoft Stream)
2. Public Administration organisations making use of the centralised digital enabling 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.
3. If the Public Administration organisation decides that the centralised digital enabling services provided by the Government are not the appropriate solutions for its needs, **alternative services** may be used. Public Administration organisations shall select the **cloud deployment model** and **service delivery model** that best suit their business.

    (The definitions being adopted for these models are those proposed by the National Institute of Standards and Technology (NIST) Definition of Cloud Computing)

    In such circumstances, a **contractual agreement** should be in place between the Public Administration organisation and the service provider which considers:

    - 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

    For systems that shall be hosted on the Agent's infrastructure:

    The system owner shall be required to justify the use of alternative services.

4. If the Public Administration organisation decides that neither the centralised digital enabling services provided by the Government 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, 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

For systems that shall be hosted on the Agent's infrastructure:

The system owner shall be required to justify the use of alternative services.

5. For security-related policy content, please refer to the GMICT Information Security Policy, especially the section related to **Asset Management**.

Electronic Payments

6. Public Administration organisations making use of the **Government Payment Gateway (GPG)** shall make use of the latest version of the GPG Developers' Toolkit[1].
7. In addition to the considerations listed in point 3 above, any **contractual agreement** for an alternative electronic payment service shall also require that the electronic payment service provider:
    - is compliant with the latest version of the PCI DSS and holds an active certification
    - is 3-D Secure enabled, where required by relevant payment methods and/or card schemes
    - uses a PCI-DSS certified hosted payment page which does not form part of the Public Administration organisation's system.
8. Government Solutions or services requiring electronic payment functionality shall provide reporting functionality in order to perform Bank reconciliations.

Notifications Service

9. Public Administration websites and software applications making use of the **Notifications Service** shall make use of the latest version of the Notification Services Development Toolkit[2].

[1] http://mita.gov.mt/gpgservice
[2] http://mita.gov.mt/notificationservice

Video Streaming Service

10. The Video Streaming Service is provided through Microsoft Stream for activities that are carried out by the Public Authority, in the exercise of **official duties**.

11. The Video Streaming Service shall **not** be used for:

    - purposes that are unlawful or constitute a security threat
    - transmitting Content that is pornographic or offensive
    - transmitting malicious Content
    - harassment, defamation or disparaging Content
    - infringement of copyright
    - personal gain, private commercial activities, or unsolicited advertising or promotional material
    - any other inappropriate purpose.

12. If an online meeting is to be recorded and the recording uploaded to the video streaming service:

    - In instances when there is a reasonable expectation of privacy, for example, **private** meetings held in personal or company offices or meeting rooms, there must be attendees' **explicit consent before** any individual may photograph, record on audio or video, or live stream the meeting or event.
    - When it may not be possible to gather each individual's explicit consent, such as at **public** meetings, hearings, or other forms of public gatherings, attendees shall be **notified before the start** of the event, and possibly even **periodically throughout** the event, that the session shall be photographed, recorded or streamed. Appropriate measures are to be taken for those who do not agree to this.
    - Rights to view any uploaded recordings shall be carefully assigned. In **Microsoft Teams**, the option **"Allow everyone in your company to view this video"** shall be **disabled**.
    - Public Authorities may seek GDPR advice and guidance from the Data Protection Unit within the Ministry for Justice, Equality and Governance.

13. When engaging third party suppliers for video conferencing services, Public Authorities should:

    - conduct a **due diligence exercise** and consider the supplier's level of information security certification, along with the supplier's reputation before engaging its services. Public Authorities should also consider whether the platform offers **end-to-end encryption**.
    - ensure that appropriate **contractual terms** (DPAs) are put in place that contain the data processing clauses set down by the GDPR.
    - consider whether to engage suppliers whose **servers are located within the European Union** to avoid having to implement additional safeguards where personal data are being transferred outside the European Union.

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 at https://rrs.gov.mt 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 **Malta Information Technology Agency**.

Contact Information

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

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