Website Policy

Reference:	GMICT P 0051	Publication:	08 January 2026
Version:	3.0	Effective:	08 January 2026

Purpose

This document covers the basic requirements for Public Administration websites.

Scope

These Policy statements apply to all Public Administration Websites that are:

- Public-facing eServices
- Web-based Information Systems (including intranets) intended for internal Government use (i.e., within and/or between Government organisations)

and for which either one of:

- a public procurement process
- internal development
- implementation of a content management system (CMS) that is immediately available for use

has not yet commenced upon the date when this policy becomes effective.

Definitions

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

Mobile first

1. A Website shall be responsive to mobile devices, **where relevant**.

Accuracy of information

2. All Website content shall be correct and timely.

Links

3. All links shall be current and not broken.
4. URL shortening to simplify URLs is allowed.

Copyright

5. A Website shall carry a Copyright Statement that declares whether there are any restrictions on the reproduction of materials published on the website.

Language

6. It is **recommended** that Website content for all public-facing Public Administration websites is provided in Maltese and English.

Advertising

7. A Public Administration organisation may add a sponsor's logo and/or website link on its Website, clearly indicating that this is an acknowledgement of sponsorship and not a general endorsement of the sponsor's commercial organisation or its activity.

Online payments

8. For online payments, reference shall be made to the GMICT Centralised Digital Enabling Services Policy.

Security

Web application security

9. A Website shall be secured and protected against the latest OWASP Top 10 Most Critical Web Application Security Risks[1], to the maximum extent possible.
10. As owner of Public Administration Websites Register, the Agent's Cybersecurity function[2] shall be informed accordingly of any commissioned or de-commissioned Website by its respective owner. Apart from the action to be taken, such information shall include the Website URL and its owner's contact details.
11. A Website shall be protected by a Web Application Firewall. Public-facing Websites that are hosted by the Agent shall be protected by a Web Application Firewall that is approved by the Agent.

[1] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[2] This is carried out via *websitesscans.mita@gov.mt*

Recommended Best Practice

CIOs are encouraged to test their websites for any weaknesses, on a regular basis in order to safeguard against security vulnerabilities identified. In conjunction with the Agent's Cybersecurity function, the use of specialised scanning tools should be applied to help identify vulnerabilities:

- prior to their official launch
- occasionally, following their launch, to protect against vulnerabilities that may arise as a result of new threats.

Reference may be made to the guides that are freely available on the OWASP Website[3], such as the:

- OWASP Developer Guide[4]
- OWASP Testing Guide[5]

12. Reference shall be made to the GMICT Information Security Policy, including for any relevant aspects of Website development .
13. Reference shall be made to the GMICT Vulnerability Disclosure Policy accordingly.
14. Appropriate corrective action shall be taken for any security vulnerability identified.

Sensitive data

15. Handling of personal data, including the use of cookies, shall comply with the General Data Protection Regulation[6], (EU) 2016/679, the Data Protection Act (CAP 586) and any other applicable legislation or regulation. Any identified breach shall be reported immediately to the appropriate authorities, which include the Data Protection Officer, Data Controller and the Information & Data Protection Commissioner.
16. Communication of sensitive information such as personal information, payment transactions and credentials, shall be protected using secure Web transport.
17. The Server Certificate used to protect sensitive information shall be:
    - Valid at time of use (i.e. not be expired)
    - Match the domain name of the website serving the sensitive information
    - Signed by an internationally-recognized Certificate Authority

[3] https://www.owasp.org

[4] https://www.owasp.org/index.php/OWASP_Guide_Project

[5] https://www.owasp.org/index.php/OWASP_Testing_Project

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1571925658226&uri=CELEX:32016R0679

Authentication

18. Websites or web services that need to authenticate using the authentication provided by the underlying platform shall use federated authentication mechanisms, in line with the GMICT Information Security Policy.

Protecting e-mail addresses

19. The publishing of personal e-mail addresses shall be avoided to the maximum extent possible, to prevent automated harvesting of e-mail addresses and the possibilities of social engineering attacks. The use of generic e-mail addresses is highly recommended.
20. Reference shall be made to the GMICT Electronic Mail Policy accordingly.

Accessibility

21. A Website shall comply with the EU Directive 2016/2102 on the accessibility of the websites and mobile applications of public sector bodies[7] (Web Accessibility Directive), the Accessibility of the Websites and Mobile Applications of Public Sector Bodies Regulations[8] (Legal Notice 89 of 2019 – CAP.418), the Equal Opportunities (Persons with Disability) Act (CAP 413, Art.13) and any other applicable legislation, regulation, directive or guidance issued by the respective authorities.

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.327.01.0001.01.ENG&toc=OJ:L:2016:327:TOC

[8] https://legislation.mt/eli/sl/418.3/eng

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, in line with GMICT Deviations from GMICT Policy Procedure.

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 https://ictpolicies.gov.mt.

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