Website Policy

Reference:	GMICT P 0051	Publication:	9 December 2019
Version:	2.0	Effective:	9 December 2019

Purpose

This document covers the basic requirements for Public Administration websites.

Scope

These Policy statements apply to all New Public Sector 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. When creating new, or updating existing websites, these are to be developed for mobile first (i.e., developed primarily for mobile devices) **where applicable** (Mobile Government Strategy 2017-2018)[1].

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 citizen-facing Government websites is provided in Maltese and English.

Advertising

7. A Ministry or Entity may add a sponsor's logo and/or a link to the sponsor's website on the Ministry or Entity 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, please refer to the GMICT Centralised Digital Enabling Services Policy.

Security

Web application security risks

9. All Public Sector websites shall be secured and protected against the latest OWASP Top 10 Most Critical Web Application Security Risks[2], to the maximum extent possible.

Recommended Best Practice

CIOs are encouraged to test their websites for any weaknesses on a regular basis in order to safeguard against the critical security vulnerabilities identified by

[1] https://publicservice.gov.mt/en/Documents/Mobile_Government_Strategy_2017-2018.pdf

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

OWASP. In conjunction with the Agent's Information Security 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]

10. For any relevant aspects of website development, such as, for example, passwords and security marking, please refer to the GMICT Information Security Policy[6].

Sensitive data

11. Handling of personal data shall comply with the General Data Protection Regulation[7], (EU) 2016/679 and any other applicable legislation or regulation.
12. Use of cookies shall comply with the Privacy and Electronic Communications Directive[8] 2002/58/EC.
13. Communication of sensitive information such as personal information, payment transactions and credentials, shall be protected using secure Web transport.
14. 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

Authentication

15. Websites or web services that need to authenticate using the authentication provided by the underlying platform shall use Web authentication, using a valid Public key infrastructure Certificate 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://mita.gov.mt/en/GMICT/GMICT%20Policies/GMICT_P_0016_Information_Security.pdf

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

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1571926645950&uri=CELEX:32002L0058

Protecting email addresses

16. The publishing of unprotected, named email addresses shall be avoided to the maximum extent possible, to prevent automated harvesting of email addresses and the possibilities of social engineering attacks. The use of generic email addresses is highly recommended.

Accessibility

Legislation

Accessibility is regulated locally by the Equal Opportunities (Persons with Disability) Act[9] (Chapter 413, Article 13) and is enforced by the Commission for the Rights of Persons with Disability[10] (CRPD).

From September 2018, **all Public Administration websites are required to conform** to the EU Directive 2016/2102 on the accessibility of the websites and mobile applications of public sector bodies[11] (Web Accessibility Directive).

This Directive was transposed into the Malta Communications Authority[12] (MCA) legal framework by means of the Accessibility of the Websites and Mobile Applications of Public Sector Bodies Regulations[13] (Legal Notice 89 of 2019). MCA is coordinating with Foundation for Information Technology Accessibility[14] (FITA) and CRPD to ensure the effective implementation of the Directive.

Deadlines and exemptions

17. The Web Accessibility Directive, Article 12 (and consequently also the Legal Notice, Article 14) requires that:
    - all Public Administration websites not published before 23rd September 2018 shall be accessible from **23rd September 2019**.
    - all other Public Administration websites shall be accessible from **23rd September 2020**.
18. The Web Accessibility Directive allows for a number of exemptions[15]. Please note that exemptions under the Web Accessibility Directive do not imply compliance with the Equal Opportunities Act, which is enforced by CRPD.

[9] https://legislation.mt/eli/cap/413/eng

[10] https://crpd.org.mt

[11] 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

[12] https://www.mca.org.mt/

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

[1414] https://fitamalta.eu

[15] https://fitamalta.eu/wp-content/uploads/2018/10/FITA-WAD-Exemptions-and-Extensions.pdf

Achieving accessibility

19. Accessibility shall be achieved by implementing the recommendations of the latest version of the Web Content Accessibility Guidelines[16] (WCAG), level AA, that enforces the ETSI standard EN301549[17]
20. Every website shall carry an Accessibility Statement, based on the model provided in the Implementing Decision (EU) 2018/1523[18]. It is recommended that accessibility statements for each website are reviewed on an annual basis.

Reference material

Practical advice on designing, producing and planning for accessible information is provided through FITA's Accessibility Certification service[19].

[16] https://www.w3.org/TR/WCAG21/

[17] https://www.etsi.org/deliver/etsi_en/301500_301599/301549/01.01.02_60/en_301549v010102p.pdf

[18] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.256.01.0103.01.ENG&toc=OJ:L:2018:256:FULL

[19] https://fitamalta.eu/fita-services/consultancy-services/

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.