GMICT Policy

ictpolicies.gov.mt

Internet Policy

Reference:	GMICT P 0091	Publication:	29 January 2019
Version:	1.0	Effective:	29 January 2019

Purpose

To regulate the use of the Internet.

Scope and Applicability

This Policy covers the use of the Internet.

GMICT Policies apply to all users of Government Information Assets, consumers of Government IT services and providers/implementers of Government Solutions.

Definitions

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

General

1. Data Controllers[1] shall enforce and ensure that their respective Ministry, Department, Secretariat or Entity implements and complies with the General Data Protection Regulation, (EU) 2016/679[2].
2. Account Holders are granted the use of the Internet on behalf of the Data Controller to perform activities that are carried out in the public interest or in the exercise of their own official authority or as delegated to them.

   Account Holders should note that Internet Account is owned by the Data Controller, who has ultimate authority over their use.
3. Government Internet shall not be used for:
   - purposes that are unlawful or constitute a security threat
   - accessing or transmitting Content that is pornographic or offensive
   - transmitting spam[3], Counterfeit E-mail or other malicious Content
   - open mail relaying purposes for messages originating from a non-Government service provider
   - harassment, defamation or derogatory statements
   - infringement of copyright
   - personal gain, private commercial activities or self-promotion
   - any other inappropriate purpose.
4. The Account Holder is responsible for the proper use of the Account. The Account Holder shall ensure that every measure is taken to avoid the possibility of unauthorised access and misuse by others.
5. Individuals shall not impersonate another Account Holder or any other individual when using the Internet.
6. An Account Holder shall only enter into or vary an agreement that legally binds the Government if they are appropriately authorised to do so. In such cases, the Account Holder shall specify that the communication is being sent "without prejudice" to any other statutory or judicial rights that the Account Holder or the Government may have.
7. Internet Accounts may be granted to non-Government individuals or organisations who have been commissioned to carry out work for or on behalf of the Government, if such a government Account is deemed necessary by the Data Controller to facilitate the fulfilment of this work. The Account shall only be used in pursuance of this work. Such individuals shall adhere to the responsibilities of an Account Holder in terms of this Policy.

[1] The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. [General Data Protection Regulation, (EU) 2016/679]

[2] The General Data Protection Regulation, (EU) 2016/679 may be found at: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[3] Unsolicited junk or bulk E-mail that is not related to work or personal interest.

8. Before sending any request for service to the Agent, the requester shall ensure that the request is correctly authorised. In such instances, the Agent fulfils the role of Data Processor[4] and shall consider all requests to have been appropriately authorised.

Monitoring and auditing

9. All Internet related activity conducted at any time by the Account Holder is subject to monitoring and audit.

10. The Agent shall keep appropriate Internet activity logs.

Audits requested by data controllers

11. The emphasis of audits requested by Data Controllers or their delegates is expected to be on the usage of the Internet service made by individual Account Holders as well as general performance of the Internet systems within their respective offices. Based on the audits carried out, the individual Data Controllers may take any action regarding individual Account Holders that they may deem appropriate. This does not exclude any action being taken outside the context of an audit.

12. The Government, through its Data Controllers, may:

    - collect and store personal information relating to the Account Holder's Internet usage. The Account Holder, through the Data Controller, may ask the Agent for access to these records kept in their regard.
    - take appropriate legal and technical action regarding Internet downloads suspected of containing inappropriate Content.

13. In cases where the Data Controller or their delegate deems that the Internet service is being misused, all related files may be used as evidence in any subsequent investigation and the following action shall be taken:

    - The Data Controller or their delegate shall inform the Account Holder that their use of the service is deemed to be inappropriate or contrary to Government Policy.
    - The Account Holder shall immediately refrain from their misuse of the service on receiving such a communication from their Data Controller. In the event that the Account Holder persists in the abusive behaviour, the Data Controller shall request the Agent to deny the Account Holder access to the relevant service, in order not to jeopardise the integrity of the system or the interests of the Government.
    - The Agent shall carry out an audit if requested by the Data Controller or their delegate.

[4] A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. [General Data Protection Regulation, (EU) 2016/679]

Audits instigated by the agent

14. The emphasis of audits instigated by the Agent shall be on the overall usage and performance of the Internet system, and not on the usage patterns of individual Account Holders. Based on the audits carried out, the Agent shall advise individual Data Controllers or their delegates on any action it may deem appropriate.

15. In cases where the Agent has a justified suspicion that the Internet service is being abused of, it may temporarily disable the Account, informing the Account Holder and Data Controller with reasons why, and carry out an audit on an ad-hoc basis.

Investigations instigated by other Competent Authorities

16. In the case of an investigation where illegal activity is suspected, the information regarding Internet usage may be disclosed by the Agent to the competent authorities without prior notification to, or consent from, the Account Holder, irrespective of the sensitivity or security classification attributed by the Account Holder to such information.

17. The Data Controller is to be notified by the Agent unless the investigating competent authority is of the opinion that such notification may prejudice the investigation being conducted.

Domains

18. All domains for Government online presences shall be registered with the Agent. All domains shall be owned by the Government.

19. The Agent shall manage the Government's Domain Name Service (DNS).

20. The gov.mt and mygov.mt domains shall be regulated by the Agent.

21. Registration of non-gov.mt domains shall follow the appropriate regulation such as the NIC Malta Domain Registration Policy[5].

22. Government websites shall make use of the gov.mt domain, unless an organisation:

    i) is an educational institution

    ii) operates upon a commercial business model

    iii) has valid business reasons to portray itself on the Internet as a non-Governmental organisation.

    in which case the domain which best suits its business strategy may be used.

23. All Government online presences, irrespective of the domain under which they are hosted, shall abide by all applicable Government ICT Policy.

[5] https://www.nic.org.mt/dotmt/

24. Government organisations requiring an online presence shall ensure that domain names selected are:

    - unique
    - representative of the name or acronym of the Government organisation, brand, function, event, etc.
    - spelt correctly in Maltese or UK English
    - easy to remember
    - easy to pronounce
    - reasonably short
    - endorsed by the CIO before requested of the Agent.

    Domain names shall also:

    - avoid infringement of, or confusion with, existing trademarks
    - not cause embarrassment to the Government organisation or the Government
    - not convey a value judgement or political statement.

Filtering

25. The Agent shall restrict access to Website categories which may potentially expose Government to security, legal, integrity[6] and/or functional[7] risks or that are deemed not to be in line with Government work.

Retention of internet activity logs

26. The Agent shall only keep activity logs for a period of 6 months.

[6] Integrity risk is the risk of damage to the corporate image of Government through unethical behaviour, e.g. viewing of pornography.
[7] Functional risk is the risk of performance degradation of Government ICT infrastructure due to the running of particular Web-related activities, e.g. download of very large files, continuous streaming, etc.

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 assessed and reported as risks.

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 can be found at **http://ictpolicies.gov.mt**.

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