Third party Web hosting services security Policy

1. Policy statement

i) General

The Government of Malta (Government) requires the secure provision of third party Web hosting services to Government Entities.

Web hosting services security requires that a third party Web hosting services provider maintains the integrity of a Government Entity’s Web site through physical and logical security at the Data Centre and on the technology deployed. Should the third party Web hosting services provider use the Agent as intermediary, then the third party Web hosting services provider shall access data through the Agent’s Demilitarised Zone (DMZ).

Web hosting services security requires that a third party Web hosting services provider establishes and maintains its own DMZ.

ii) Web hosting server technology

Web hosting server technology for third party Web hosting services to a Government Entity shall be subject to the following: (i) the Web hosting server technology shall operate from a Data Centre that is physically located in Malta, that is secure and that guarantees logical information security, based on European recognised standards as specified in the Supporting Documents section of this Policy (ii) the Web hosting server technology shall be equipped for business continuity purposes, and (iii) the administration of the Web hosting
server technology shall require documented security procedures that shall be available for audits.

iii) Network

The network between the third party Web hosting services provider and the Government Entity shall be secure from unauthorised access.

iv) Implementation

The target population are: (i) Government Entities and (ii) third party Web hosting services providers.

Implementation from a security point of view shall be backed by:

(i) A Service Level Agreement, between the third party Web hosting services provider and the Government Entity, that shall comply with this Policy.

(ii) A Declaration of Security Conformance, issued by the third party Web hosting services provider to the Government Entity, copied to CIMU. This Declaration shall be used as another reference for the selection of a third party Web hosting services provider. It shall be the responsibility of the third party Web hosting services provider to ensure, on an on-going basis, that services provided via an Internet services provider are subject to the Declaration of Security Conformance.

(iii) Internal security audits, by the third party Web hosting services provider on its operations, for Security Conformance purposes. Records shall be maintained in the process. The third party Web hosting services provider shall carry out timely and effective follow-up action to satisfactorily close items arising in the internal security audits. The third party Web hosting services provider shall maintain records of the actions taken.

(iv) Security Compliance checks, by CIMU on the third party Web hosting services provider. CIMU shall maintain records in the process. The third party Web hosting services provider shall carry out timely and effective follow-up action to satisfactorily close items arising in the external security audits. The third party Web hosting services provider shall maintain records of the actions taken.


v) Policy violations

Abuse or misuse of third party Web hosting services by the Government Entity and/or the third party Web hosting services provider in terms of the Telecommunications (Regulation) Act, Electronic Commerce Act, the Data Protection Act and the Computer misuse provisions of the Criminal Code shall be treated as an offence.
2. **Purpose**

The objective of this Policy is to ensure that third party Web hosting service providers provide secure third party Web hosting services to Government Entities.

3. **Who should know this Policy**

Knowledge of this Policy should extend up and down the organisations concerned and be wide spread within them.

- Chief Information Management Officer (CIMO)
- CIMU Communications Executive
- Head of Agent
- Ministry of Justice and Local Government
- Information Management Officers (IMOs)
- Head of Government Entity
- Head of Third party Web hosting services provider
- Head of Internet services provider
- Head of MCA

4. **Scope of applicability**

The provisions of this document apply to the security of third party Web hosting services provided to Government Entities by third party Web hosting services providers that (i) operate the services through the Agent or independently and (ii) host Web sites published under the `gov.mt` domain.

5. **Definitions**

**Agent** - a trusted organisation that has the mandate by Government to provide Information and Communications services.

**Computer network** - a network of data processing nodes that are interconnected for the purposes of data communication.

**Data Centre** - a facility that includes personnel, hardware and software organised to provide information processing services.

**Declaration of Security Conformance** - a documented statement issued by the third party Web hosting service provider to the Government Entity; by which the third party Web hosting service provider declares, under its sole responsibility, conformance to this Policy. In the event that the third party Web hosting services provider does not act as an Internet services provider, the Declaration of Security Conformance shall also cover the Internet services provider that provides services to the third party Web hosting services provider. The
Declaration shall also include the reference number of registration with the MCA. This Declaration shall be considered as separate from the Declaration of Conformance.

**Demilitarised Zone (DMZ)** - the organisation’s "neutral zone" between the organisation’s computer network and the external network to prevent outside users from getting direct access to internal computer servers that have data. Outside users can only have access to the DMZ that may typically also have Internet resources that could be served to the outside world.

**Government Entity** - a Government Ministry, Department, Local Government or Public Sector entity.

**Security Compliance** - the process performed by CIMU or by an independent body to check that a service provided satisfies the security criteria set in a referenced document.

**Security Conformance** - the correspondence by a service to the security criteria set in a referenced document.

**Third party Web hosting service** - the process in which a third party services provider furnishes a Government Entity with a Web site presence.

**Third party Web hosting service provider** - a local private organisation having a physical Web hosting presence under Maltese jurisdiction and be compliant with the applicable authorisation requirements of the MCA.

### 6. Roles and responsibilities

For the purpose of this Policy, the following roles and responsibilities have been identified:

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibility</th>
</tr>
</thead>
</table>
| 1. Chief Information Management Officer (CIMO) | i. To maintain this Policy.  
ii. To audit for security compliance. |
| 2. CIMU Communications Executive | i. To publish this Policy.  
ii. To liaise appropriately with the Agent with regards to the publication of this Policy on the CIMU Website. |
| 3. Head of Agent | i. To establish and maintain the DMZ. |
4. Head of Government Entity
   i. To direct the Government Entity according to the provisions found in this Policy.
   ii. To grant access to the Government Entity's Web site once the appropriate controls have been implemented and the terms for connection or access have been defined and agreed upon in a contractual agreement.

5. Head of third party Web hosting services provider
   i. To have a publicly declared target dates to achieve accredited certification to MSA BS 7799 Part 2:2003 for the scope of applicability of this Policy.
   ii. To operate Web hosting services according to the provisions of this Policy.
   iii. To establish and maintain its own DMZ.
   iv. To audit for Security Conformance.
   v. To conduct timely and effective follow-up action to satisfactorily close items arising in internal and external security audits.
   vi. To keep updated on vulnerabilities that effect the Web hosting services environment and have the latest security fixes in place.

6. Head of Internet services provider
   i. To operate according to the provisions of the Declaration of Security Conformance issued by the third party Web hosting services provider.

7. Supporting Documents

In support of this Policy, the following Standard shall apply:


8. References

01. The Telecommunications (Regulations) Act – Chapter 399
    http://www.justice.gov.mt

02. Data Protection Act – Chapter 440
    http://www.justice.gov.mt

03. Electronic Commerce Act – Chapter 426
9. Modification history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>19.06.2002</td>
<td>Initial release</td>
</tr>
<tr>
<td>2.0</td>
<td>09.04.2003</td>
<td>Updated release</td>
</tr>
</tbody>
</table>

10. Maintenance and review cycle

Maintenance of this Policy shall be based on a twelve month cycle.

Signature and stamp

Joseph R. Grima

Permanent Secretary, Office of the Prime Minister