Vulnerability Disclosure Policy

GMICT Policy – GMICT P 0122

Purpose

Provides direction and endorsement for **vulnerability disclosure** and related activities conducted in **good faith**.

Applies to **researcher(s)** testing systems owned by the **Agent (MITA) and Government.**

The Agent prioritizes **safeguarding Government data and services** against cyber threats using advanced security infrastructure.

The **Government CSIRT oversees** security matters, including vulnerability disclosures.

Recognizes that **no system** is completely **foolproof** and supports **continuous** security improvements.

Acknowledges **contributions** from the cyber-research community to enhance the **security of public-facing systems**.

Scope

Applies to researchers conducting **good-faith vulnerability research**.

Covers **public-facing systems** owned by the **Agent or Government**.

Only applies if a **security.txt** file exists at **<domain>/.well-known/security.txt**.

Any system **not meeting these criteria** is **out of scope** and **not authorized**.

Non-compliant activities are **excluded** and **not endorsed**.

Research and Testing

Researches shall refrain from engaging in:

- Violating privacy rights
- Degrading user experience
- Disrupting systems
- Destroying or manipulating data
- Activities that contravene the established law or that may lead to the Agent, Government, or their partner organisations to be in breach of any legal obligations.

Research and Testing

The scoping of **testing activities** shall be proportionate to **confirming the presence of a vulnerability**.

The use of **exploits** is **prohibited** for the following:

- Illegally extracting or exfiltrating data
- Opening, copying, or deleting files
- Utilising and exploiting command line access
- Pivoting to other systems

Research and Testing

Researchers cannot perform:

Social engineering and/or Denial of Service (DoS or DDoS)

Escalate privileges or move laterally within the network

Disrupt Services provided by the Agent and Government third party suppliers

Introduce Malware or any form of malicious code

The General Data Protection Regulation, (EU) 2016/6791 and the Data Protection Act (CAP 586) shall be adhered to

Infringement of The General Data Protection Regulation, (EU) 2016/6791 and the Data Protection Act (CAP 586)

Their obligations

Any data retrieved during research and testing shall be securely deleted as soon as it is no longer required or within one month of the vulnerability being resolved, whichever comes first

Reporting

Upon confirmation of the existence of a vulnerability:

- Testing shall be immediately halted,
- **govmtCSIRT shall be promptly notified** of any **discovered vulnerability**, whether **real** or **potential**, within **seventy-two (72) hours** of its identification.
- **No associated** information shall be **disclosed to third parties** or to the **general public.**
- Reported vulnerabilities **shall not be disclosed without coordination** with govmtCSIRT.

Testing shall be **immediately halted**, **govmtCSIRT shall be informed**, and **no associated** information shall be **disclosed**, **in case of encounter of the following types** of information during testing:

- **Personally Identifiable Information**
- **Financial information**
- **Proprietary information** or **trade secrets** belonging to any party
- **Classified Government information**
- **Gained command line access**

Report Structure

Section	Mandatory?	Description
Email to:	Yes	mt-csirt@gov.mt
Title	Yes	A short description of the vulnerability. E.g. Admin privileges through cross site scripting
Affected Asset	Yes	The asset that has the vulnerability such as web address, IP address, service or product name
Weakness	Yes	A description of the weakness. Preferably follows the CVW format https://cwe.mitre.org/ https://cwe.mitre.org/data/definitions/699.html https://cwe.mitre.org/data/definitions/1194.html
Impact	No	In your opinion list the severity of the impact on MITA and the Maltese Government. Low: The vulnerability has minimal impact on MITA and the Maltese Government. Medium: The vulnerability has a significant impact on MITA and the Maltese Government. High: The vulnerability has a serious impact on MITA and the Maltese Government. Critical: The vulnerability has a detrimental impact on MITA and the Maltese Government.
CVSS Score	No	Calculate, in your opinion the CVSS score via https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
Description of the vulnerability	Yes	• A summary of the vulnerability • Supporting files (e.g. screenshot or video) • Any mitigations or recommendations
Steps to Reproduce	Yes	• Clear and descriptive steps to reproduce the vulnerability • Proof of concept code if available
Contact Details	Yes	Name Surname Mobile Number Email

Response

govmtCSIRT shall **issue a report** indicating the **true impact** and **CVSS scores**.

govmtCSIRT shall **respond** to **researchers' reports** within **five (5) working days** and provide a **preliminary assessment** within **ten (10) working days**.

govmtCSIRT is bound to **keep the researcher(s) informed** throughout the process of addressing the vulnerability.

Prioritisation of the vulnerability by the Agent shall be based upon the following:

- The **impact** of the vulnerability
- The **complexity** of exploiting the vulnerability
- The **likelihood** of the vulnerability being exploited

The Agent shall classify the vulnerability according to severity. The severity and its associated definitions the expected time for remediation.

Remediation

Severity	Description	Time for remediation
Low	A vulnerability if exploited poses minimal or negligible harm to the Agent, Government, and their partner organizations	One (1) year
Medium	A vulnerability if exploited will result in substantial harm to the Agent, Government and their partner organizations.	One hundred and eighty (180) days
High	A vulnerability if exploited, will inflict extensive harm to the Agent, Government and their partner organizations.	Ninety (90) days

Response

The researcher(s) shall refrain from inquiring on the status of the vulnerability remediation more than once every fourteen (14) working days.

The Agent shall **inform** the researcher(s) accordingly when the **reported vulnerability** has been **remediated** and may **invite** them to confirm that the vulnerability has been **adequately addressed**.

The researcher(s) **may submit a request to disclose the report**, after the vulnerability has been successfully resolved.

Current Status

- Deployed on MITA site
- Deployed on WoPHoP sites
- Being deployed on all MITA managed sites

Way forward

Deployment of security.txt file on any public-facing system by **1st May 2025**.

Once deployed, respective IMUs shall:

- keep a record;
- inform immediately **govmtCSIRT** by sending an email to govmtCSIRT@gov.mt with the following details:

Date Implemented	Domain	Hosting Platform	Project/Service Owner	Contact Person	Department/Unit
01/03/2025	www.domain.mt	AWS , GoDaddy etc	Mr Joseph Tedesco – OPM	imu.opm@gov.mt – Phone number	OPM - IMU

CIOs and IMU offices are vital to **collaborate** with **MITA** for any enquires based on the VDP and shall do their utmost to ensure the adherence with timeframes.

References:

https://mita.gov.mt/wp-content/uploads/2025/03/GMICT_P_0122_Vulnerability_Disclosure.pdf

mita

Thank You