# Vulnerability Disclosure Policy

| | | | |
|---|---|---|---|
| Reference: | GMICT P 0122 | Publication: | 17 March 2025 |
| Version: | 1.1 | Effective: | 17 March 2025 |

## Purpose

This policy aims to provide clear direction and endorsement on vulnerability disclosure and associated activities, including research and testing, conducted in good faith by researcher(s) on systems owned by the Agent and Government.

The Agent is committed to safeguard Government data and services from escalating cyber threats, through its implementation of cutting-edge security infrastructure. To ensure comprehensive security oversight, it actively monitors and coordinates security matters within Government infrastructure through govmtCSIRT - the Government CSIRT. Such coordinating role shall also pertain to vulnerability disclosures, through this Policy.

Ultimately, through this Policy, Government is reaffirming its belief in continuous security improvements, based upon the premise that systems can never be completely fool proof. Furthermore, Government is also recognising related potential contribution by the cyber-research community and individual researcher(s) to its public-facing systems, as reflected within the **Scope** of this Policy.

## Scope

This Policy applies to researcher(s) engaging in good-faith vulnerability research activities on public-facing systems owned by the Agent or Government and which have a security.txt file located at <domain>/.well-known/security.txt.

Any system not as specified above is excluded from the **Scope** and is therefore not authorised for vulnerability research activities.

Activities not conformant to the provisions of this Policy are excluded and therefore not endorsed.

## Definitions

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

# Research and Testing

## Rationale

The following are the Policy provisions expected of the researcher(s), during the conduct of the research and testing activities.

1. Every effort shall be made to 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.
2. 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.
3. Social engineering and/or Denial of Service (DoS or DDoS) attacks are not allowed.
4. No attempt shall be made to escalate privileges or move laterally within the network.
5. Services provided by the Agent and Government third party suppliers shall not be disrupted.
6. Malware or any form of malicious code shall not be introduced.
7. The General Data Protection Regulation, (EU) 2016/6791 and the Data Protection Act (CAP 586) shall be adhered to. The infringement upon the privacy of individuals, organisations, systems or services associated with the Public Administration, including the Agent, shall be avoided. The sharing, redistributing or the inadequate securing of any such data obtained shall not be allowed.
8. 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

### Rationale

govmtCSIRT has the sole responsibility for coordinating all vulnerability disclosure activities on the Agent and Government systems.

The following are the Policy provisions, including obligations from the researcher(s). when reporting to govmtCSIRT.

9. Upon confirmation of the existence of a vulnerability, testing shall be immediately halted, govmtCSIRT informed, and no associated information shall be disclosed to third parties or to the general public.
10. govmtCSIRT shall be promptly notified of any discovered vulnerability, whether real or potential, within seventy-two (72) hours of its identification.
11. The security vulnerability shall be reported to govmtCSIRT, using the structure as shown in **Appendix 1.**
12. Reported vulnerabilities shall not be disclosed without coordination with govmtCSIRT.
13. 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
    - Gaining command line access.

## Response

### Rationale

The following are obligations from the researcher(s) and expectations of the Agent in response to vulnerability disclosures.

14. After a vulnerability reported to govmtCSIRT is assessed, the Agent shall issue a report indicating the true impact and CVSS scores. The Agent's report shall be the final indication of the severity of the vulnerability.
15. The Agent shall respond to researchers' reports within five (5) working days and provide a preliminary assessment within ten (10) working days. The Agent shall strive to keep the researcher(s) informed throughout the process of addressing the vulnerability.
16. 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.

17. The Agent shall classify the vulnerability according to severity. The severity and its associated definitions and expected time for remediation is as follows:

| 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 |

18. 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 them accordingly when the reported vulnerability has been remediated and may invite them to confirm that the vulnerability has been adequately addressed.
19. The researcher(s) may submit a request to disclose the report, after the vulnerability has been successfully resolved.

## Best Practice

The Agent encourages researcher(s) to coordinate the public release of information along with it, as it provides the opportunity for a unified and coherent message of guidance to the relevant stakeholders.

# Appendix 1: Structure of report to be used when informing govmtCSIRT of a vulnerability discovered.

| Section | Mandatory? | Description |
|---|---|---|
| Email to: | Yes | govmtCSIRT@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<br>https://cwe.mitre.org/ https://cwe.mitre.org/data/definitions/699.html<br>https://cwe.mitre.org/data/definitions/1194.html |
| Impact | No | In your opinion list the severity of the impact on the Agent and the Maltese Government.<br>Low: The vulnerability has minimal impact on the Agent and the Maltese Government.<br>Medium: The vulnerability has a significant impact on the Agent and the Maltese Government.<br>High: The vulnerability has a serious impact on the Agent and the Maltese Government.<br>Critical: The vulnerability has a detrimental impact on the Agent 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<br>• Supporting files (e.g., screenshot or video)<br>• Any mitigations or recommendations |
| Steps to Reproduce | Yes | • Clear and descriptive steps to reproduce the vulnerability<br>• Proof of concept code if available |
| Contact Details | Yes | Name<br>Surname<br>Mobile Number<br>Email |

## Conformance to this Policy

Any activity by the researcher(s) beyond the **Scope** of this Policy shall be subject to legal prosecution.

No legal action shall be taken by the Agent if the researcher(s) conform to the provisions of this Policy. The Agent may take steps to make the conformance known if legal action is instituted by a third party against such researcher(s).

However, legal action shall be taken by the Agent against researcher(s) who attempt to hold it to ransom, even if they are operating within the **Scope** of this Policy.

## Issuing Authority

This document has been issued by the **Principal Permanent Secretary**.

## Contact Information

Government ICT Policies may be found at **http://ictpolicies.gov.mt**.

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