
NATIONAL DATA
MANAGEMENT AUTHORITY

# Malware Incident Prevention Policy

**Prepared By:**

**National Data Management Authority**
**March 2023**

**Document Status Sheet**

| | Signature | Date |
|---|---|---|
| **Policy Coordinator (Cybersecurity)** | **Muriana McPherson** | **31-03-2023** |
| **General Manager (NDMA)** | **Christopher Deen** | **31-03-2023** |

**Document History and Version Control**

| Date | Version | Description | Authorised By | Approved By |
|---|---|---|---|---|
| **31-03-2023** | **1.0** | | **General Manager, NDMA** | **National ICT Advisor** |

**Summary**

1. This policy addresses the acceptable mechanisms to prevent malware incidents.
2. This is a living document which will be updated annually or as required.
3. Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

## 1.0 Purpose and Benefits

The purpose of this policy is to define rules for deploying and maintaining mechanisms to prevent malware incidents on the Government of Guyana's (GoG) Networks.

## 2.0 Authority

The Permanent Secretary, Administrative Head, Head of Human Resources or their designated representative of the Public Sector Organisation is responsible for the implementation of this policy. For further information regarding the foregoing, please contact the Policy Coordinator - National Data Management Authority (NDMA).

## 3.0 Scope

This policy applies to all users of Information systems and encompasses all systems, automated and manual, for which the Government of Guyana has administrative responsibility, including systems managed or hosted by third parties on behalf of the Government. It addresses all information, regardless of the form or format, which is created or used in support of business activities. It is the user's responsibility to read and understand this policy and to conduct their activities in accordance with its terms. In addition, users must read and understand the organisation's Information Security Policy and its associated standards.

## 4.0 Policy

The presence of malware on the Government of Guyana's network can threaten the confidentiality, integrity, and availability of data on the network, which can ultimately hinder staff productivity and result in data, reputational and financial loss, unplanned system and network downtime and unauthorised disclosure and modification of information. This policy aims at protecting the Government of Guyana's information systems and its networks from malware.

### 4.1 General

4.1.1 Every Ministry/Agency is required to maintain a list of Organisation approved malware protection solutions to be installed on computer systems connecting to their networks. Each employee will be expected to conform to using the list of approved malware protection solutions.

4.1.2 All computer systems connecting to the Organisation's network must have licensed, up-to-date malware protection solutions installed that offer real-time scanning protection to files and applications running on the target system.

**4.2** Each ministry / agency shall configure their malware protection solutions so that they:

4.2.1 automatically update endpoint computer systems regularly

4.2.2 automatically remove viruses and quarantine those that cannot be removed

4.2.3 disable autorun, auto-play and auto-execute functionality for removable media

4.2.4 automatically scan removable media

4.2.5 block users from accessing websites with known malware and warn users who are attempting to access suspicious websites.

**4.3** Malware protection solutions shall not be disabled during computer systems and data backups.

**4.4** Where possible, the use of behaviour-based anti-malware solutions is encouraged.

**4.5** Where possible, agencies are recommended to implement malware protection solutions which can be centrally managed.

**4.6** Employees are prohibited from making any modifications to malware protection solutions (such as disabling or tampering). Such changes are only to be done by authorised members of the IT Division of the respective ministry/agency when necessary.

**4.7** Mail servers in use must have malware protection solutions that scan all e-mails to and from the mail server and filter suspicious e-mails.

**4.8** Each agency must employ an appropriate awareness program to encourage users to exercise caution when opening e-mails or attachments.

**4.9** Each agency shall be responsible for ensuring that all critical malware incidents occurring at the agency are logged and reported to the National Data Management Authority as per the Office of the Prime Minister correspondence dated 16th June 2023. See Appendix A "Cybersecurity Incident Reporting System"

**4.10** All activities to create and/or distribute malicious software onto the Government of Guyana's network are strictly prohibited.

**4.11** If deemed necessary to prevent propagation to other networked computer systems or detrimental effects to the network or data, an infected computer system may be disconnected from the Government of Guyana's network until the infection has been removed.

**4.12** No employee shall attempt to destroy or remove malware, or any evidence of that malware, without direction from the IT division of the agency and Incident Handling personnel. Of note, such direction may exist in documented organisational approved procedures.

## 5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all organisational policies and standards. Failure to comply with the policy may, at the full discretion of the Permanent Secretary, Administrative Head, or Head of Human Resources of the Public Sector

Organisation, result in the suspension of any or all privileges and further action may be taken by the Ministry of Public Service.

## 6.0 Exceptions

Requests for exceptions to this policy shall be reviewed by the Permanent Secretary, Administrative Head, Head of Human Resources of the Public Sector Organisation, or the Policy Coordinator, NDMA. Departments requesting exceptions should provide written requests to the relevant personnel. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a timeframe for achieving the minimum compliance level with the policies set forth herein.

## 7.0 Maintenance

The Policy Coordinator, NDMA shall be responsible for the maintenance of this policy.

## 8.0 Definition of Key Terms

| Term | Definition |
|---|---|
| **Computer System[1]** | Means a device or group of interconnected or related devices, which follows a computer programme or external instruction to perform automatic processing of electronic data; and<br>Includes, but is not limited to, a desktop computer, a laptop computer, a netbook computer, a tablet computer, a video game console, internet connected devices, a smart phone, a personal digital assistant, a smart television or a video camera. |
| **Malware [2]('malicious software')** | A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting theF victim. |
| **Virus[3]** | A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. |
| **Worms[4]** | A computer program or algorithm that replicates itself over a computer network and usually performs malicious actions. |

[1] *Retrieved from*: Laws of Guyana, Cybercrime Act 2018, N0.16 of 2018

[2] *Retrieved from* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/user

[3] *Retrieved from* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/user

[4] *Retrieved from* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/user

## 9.0 Contact Information

Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.