NM DEPARTMENT OF
INFORMATION
TECHNOLOGY

**Michelle Lujan Grisham**
New Mexico Governor

**Raja Sambandam**
Acting Cabinet Secretary & State CIO

| | |
|---|---|
| **Policy Title:** | **Anti-Malware/Virus Policy** |
| **Policy Number:** | **DoIT-361-702** |
| **Effective Date:** | 6/27/2022 |
| **Issued By:** | **DoIT CIO** |
| **Distribution:** | **DoIT IT Resource Users** |
| **Approved by:** | **Raja Sambandam, Acting Cabinet Secretary** |

## 1. AUTHORITY

Pursuant to the New Mexico Department of Information Technology Act, NMSA 1978, § 9-27-1 *et seq.*, the Secretary of the Department of Information Technology (DoIT or Department) shall exercise general authority over all department employees, manage all operations of the Department, and administer and enforce the laws with which the Secretary or Department is charged.

Pursuant to NMAC 1.12.20, DoIT is responsible to implement controls to detect and prevent any computer virus and other malicious code from being introduced to the agency environment.

## 2. PURPOSE

This Policy provides direction and minimum requirements for establishing anti-malware protectionsfor DoIT personal computers (PC's), laptops, servers, and mobile devices.

## 3. SCOPE

This Policy is applicable to all DoIT PC's, laptops, servers, and mobile devices (collectively, "Devices"). It applies to all DoIT Information Technology (IT) Resource Users.

## 4. DEFINITIONS

a. **DoIT IT Resource Users** - All DoIT employees, vendors, contractors, and other users of DoIT IT resources.

b. **Anti-Malware/Virus Software** – Software designed to detect, contain, or otherwise eradicate malicious code.

c. **Virus** – A computer program, typically hidden within another seemingly innocuous program,that produces copies of itself and inserts them into other programs, usually to perform a malicious action (such as destroying data).

d. **Malware** – Software designed to interfere with a Device's normal operating function.

## 5. POLICY

DoIT will install and maintain appropriate anti-malware/virus software to protect the agency's data integrity and security. DoIT mandates all Devices,information system entry and exit points, and any other systems that are commonly affected by malicious software (*e.g.*, mail servers, web servers, proxy servers, remote-access servers, etc.) meet this requirement. Anti-malware/virus scanning software definition updates must be real time and must be pushed to clients daily.

Users may not disable any active anti-malware software. Users must never open or download any files attached to an email from an unknown, suspicious, or untrustworthy source. As soon as a useridentifies a malicious e-mail, they must delete the message from their inbox, as well as any spam, chain, or other junk emails.

Anti-malware/virus software on all Devices must check for updates at each login or connection. All Devices must be scanned automatically in real time, and full scans must run at least once a week on all workstations and servers. Before being introduced on DoIT IT resources, all software code and files must be scanned for viruses.

DoIT maintains anti-malware/virus protection software audit logs and software activity logs for at least ninety (90) calendar days. Before using or transferring files from a removable media device (*e.g.*, USB device, thumb drive, CD, DVD) connected to a DoIT Device, the removable media device must first be scanned with the anti-malware scanner.

### 5.1. Virus Incidents

All malicious code infections must be treated as security incidents and be handled in accordance with the DoIT *Incident Management and Response Policy*. All DoIT users are required to report virus incidents to the DoIT Helpdesk, which will log the incident in accordance with the DoIT *Incident Management and Response Policy*. The DoIT Helpdesk team will isolate the infected computer, determine if the threat is valid, and remove the threat or escalate the issue to the security team as needed. If the virus caused any damage to the workstation/server, the responsible system administration staff must restore the infected device to its original state before it is returned to use.

## 6. ROLES AND RESPONSIBILITIES

### a. DoIT CISO

The DoIT Chief Information Security Officer (CISO) or Chief Information Officer (CIO) designee will ensure that approved anti- malwaresolutions are active, effective, and maintained as directed in this Policy.

The DoIT Security Team is responsible for reviewing scan results and logs daily, and for ensuring definition updates occur as required. The DoIT Security Team must receive anti-malware system notifications and respond to alerts as soon as possible.

### b. DoIT IT Resource Users

All DoIT IT Resource Users must adhere to this Policy and must maintain anti-malware/virus systems as required.

Users are responsible for awareness of the processes and procedures for dealing with virus incidents.

If a user suspects infection by a virus or malware, the user must shut down the involved Device, disconnect from all networks, and obtain assistance from the DoIT Helpdesk.

Contractors, consultants, vendors, temporary staff, and any other individuals working with DoIT systems are required to have up-to-date anti-virus protection software on their Devices.

## 7. EXCEPTIONS

The DoIT CIO or CISO must approve any exception to this Policy in writing.

## 8. VIOLATIONS OF POLICY

Any DoIT IT Resource User found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.

## 9. REFERENCES

a. 1.12.20 NMAC

b. Payment Card Industry Data Security Standards v3.2: Requirement 5

c. National Institute of Standards and Technology, Security and Privacy Controls for Federal Information Systems, SP800-53 r4: MA-3(2), MA-6(3), SI-2, SI-3, SI-3(1), SI-3(2), SI-4, SI-4(2),

d. International Organization for Standardization/International Electrotechnical Commission Information Systems Audit and Control Association: Controls Objectives for Information and Related Technologies v5.0

e. Department of Information Technology Incident Management and Response Policy

## 10. CHANGE HISTORY

| Date | Version | Changed By | Change Comments |
|---|---|---|---|
| 09/30/2019 | 1 | | Initial Draft |
| 09/30/2020 | 2 | | Revision Draft |
| 02/26/2021 | 3 | Raja S | Revised and routed for Union approval |
| 05/13/2021 | 4 | Olga Serafimova, Esq. | Reviewed and revised for legal compliance |
| 10/13/2021 | 5 | Brenda Fresquez | Reviewed for quality assurance |

## Approval

DocuSigned by:
437214FBE82C453...

6/27/2022

**Raja Sambandam, Acting Cabinet Secretary** **Date**