NM DEPARTMENT OF
INFORMATION
TECHNOLOGY

Michelle Lujan Grisham
New Mexico Governor

Raja Sambandam
Acting Cabinet Secretary & State CIO

Policy Title:	**Patching and Updating Policy**
Policy Number:	**DoIT-361-712**
Effective Date:	**June 14, 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 the Department is charged.

Pursuant to 1.12.12.8(C), commercial software applications must come with an established timely schedule for new version updates and bug fixes.

Pursuant to 1.12.20 NMAC, tools used to scan for vulnerabilities shall be updated at least quarterly to ensure any recently discovered vulnerabilities are included in any scans; tools used to perform penetration testing shall be kept updated to ensure that recently discovered vulnerabilities are included in any future testing; and virus signature files shall be kept updated by the agency system administrator for most agency workstations, whereas on host systems or servers, the signature files shall be updated when the virus software vendor's signature files are updated and made available.

2. PURPOSE

This policy provides direction on reviewing and implementing patches for operating systems, applications, network devices and other IT resources. Identifying and applying critical and relevantupdates and patches helps protect DoIT IT resources, maintain compliance with regulations, protect critical information, and reduce business risks. This Policy establishes a process and schedule for patching and updating DoIT IT resources.

3. SCOPE

This Policy applies to all operating systems, network devices, and applications that DoIT maintains.

4. DEFINITIONS

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

b. **Patch** – A piece of software designed to update a computer program or its supporting data, including fixing security vulnerabilities and other bugs.

c. **Update –** A process of bringing something up to date, or an updated version of something tomake something more modern or current.

d. **User Acceptance Testing –** The process of verifying a software update is functional and working as desired for application or system use.

5. POLICY

DoIT uses various operating systems, network devices and applications (software) to conduct business activities. Vendors periodically release patches to mitigate vulnerabilities or issues found within the associated software. All computer systems (operating systems, software, firmware) usedat DoIT must be maintained and current with relevant patches and updates.

DoIT's patch management process includes:

- **a.** Monitoring and identifying new patches and updates;
- **b.** Evaluating the risk associated with patches and updates in relation to critical systems and the organization;
- **c.** Testing processes for all patches and updates;
- **d.** Detecting missing patches and updates and using tools such as vulnerability scanners;
- **e.** Tracking all patches and updates against inventoried components;
- **f.** Scheduling patch management and upgrades, including a regular bi-weekly patch and update cycle; and
- **g.** Following the formalized *IT Change Management Policy* and testing processes for allpatches and updates implementations.

5.1. Analysis

DoIT System Administrators monitor release of patches or updates for their assigned systems. Responsible staff evaluate new patches and updates for risk level (vendor perspective and DoIT perspective). Staff will implement "critical" or "important" patches within five (5) business days of release and will schedule testing and implementation within a reasonable timeframe based upon riskexposure. Staff will deploy "non- critical" or "low risk" patches or upgrades within three (3) months of their release.

5.2. Testing

All patches must be tested prior to implementation into the production environment to ensure systems and applications continue to work properly after patches are implemented. After testing is completed and the patch or update is implemented in the production environment, responsible staff must verify that no anomalies occur due to the change. If a patch cannot be introduced to the production environment, responsible staff shall put in place mitigating controls to protect the affected system from the vulnerability the patch is intended to mitigate**.**

5.3. Recovery/Back out

If a deployed patch or update causes instability, responsible staff must uninstall and back outthe patch or update following back-out or uninstall procedures documented during the change control process. A last known good configuration is necessary to perform a rollback to remove the patch from the environment. The previous configuration shall be retained until a new stable configuration has been verified.

6. ROLES AND RESPONSIBILITIES

a. DoIT CISO

The DoIT Chief Information Security Officer (CISO) or Chief Information Officer (CIO) designee is responsible for the overall organizational adherence to this Policy and may request an audit of systems at any point in time to ensure compliance.

b. DoIT System Administrators

i. Monitor sources (e.g., websites, mailing lists, vendor updates) to identify new patches;

ii. Review released patches for their assigned systems and applications;

iii. Assess patch criticality;

iv. Review patch notes to understand the purpose and how it applies to DoIT systems;

v. Follow the change control process for submitting patches and the back out plan with last best-known system states; and

vi. Schedule and conduct patch implementation and testing.

7. EXCEPTIONS

The DoIT Chief CIO or DoIT CISO must approve in writing any exceptions to this policy.

8. VIOLATIONS OF POLICY

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

9. REFERENCES

a. Payment Card Industry Data Security Standards v3.2: 6.1, 6.2

b. National Institute of Standards and Technology SP800-53 r4: SI-2

c. International Organization for Standardization/International Electrotechnical Commission 27002:2013: 12.6.1, 12.1.2

10. CHANGE HISTORY

Date	Version	Changed By	Change Comments
09/30/2019	1		Initial Draft
09/30/2020	2		Revision Draft
05/27/2021	3	Olga Serafimova, Esq.	Reviewed and revised for legal compliance
4/27/2022	4	Brenda Fresquez	Reviewed for quality assurance
12/18/2023	4.1	Brenda Fresquez	Annual Review; updated header and footer
12/18/2023	4.1	Bryan E. Brock	Annual Review for legal compliance; no recommended changes

Approval

DocuSigned by:

437214FBE82C453...

12/20/2023

Raja Sambandam, Acting Cabinet Secretary

Date