NM DEPARTMENT OF INFORMATION TECHNOLOGY

Michelle Lujan Grisham
New Mexico Governor
Raja Sambandam
Acting Cabinet Secretary & State CIO

Policy Title:	**Vulnerability Management and Assessment Policy**
Policy Number:	**DoIT-361-718**
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.

Per 1.12.20.24 NMAC, all state computing infrastructures that provide information through a public network, either directly or through another dedicated circuit, and that provide information externally, shall be subject to annual independent penetration analysis and intrusion testing by qualified, independent third-party contractor approved by DoIT.

2. PURPOSE

This Policy presents requirements for implementing and maintaining a vulnerability assessment and penetration testing methodology to proactively identify and mitigate system vulnerabilities in operating systems, network components, applications, and other DoIT computer systems.

3. SCOPE

This Policy applies to internal DoIT staff and third-party contractors managing vulnerabilities for all DoIT IT systems and resources.

4. DEFINITIONS

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

b. **Vulnerability Assessment –** The process of identifying technical vulnerabilities in IT assets and networks and identifying weaknesses in policies and practices relating to operation of these systems.

c. **Penetration Testing –** An authorized simulated attack on a computer system performed to evaluate the system's security.

5. POLICY

DoIT will implement and maintain vulnerability assessment and penetration testing methodologies to proactively identify security vulnerabilities and to mitigate them in a timely and effective manner. The purpose of these methodologies, and associated tools, is to help ensure the continued security and protection of DoIT IT assets, including systems, networks, data, and facilities.

Vulnerability assessment and testing methods will include, at a minimum:

a. Subscribing to and monitoring vendor, security, and other "alerting list" organizations for new vulnerability alert announcements and analyzing those alerts

b. Performing, at a minimum, quarterly internal and external vulnerability assessments on critical servers, network components, and applications

c. Retaining third-party security consultants to perform annual internal and external penetration testing on critical servers, network components, and applications

d. Performing internal and external vulnerability assessments or penetration testing after any significant changes in network or applications; and

e. Documenting and implementing a vulnerability assessment and penetration testing methodology based on industry-accepted testing approaches, such as National Institute of Standards and Technology (NIST) SP800-115: Technical Guide to Information Security Testing and Assessment.

5.1 Vulnerability Assessments

Vulnerability assessment processes and procedures will be established and performed at least quarterly or after any major changes to the infrastructure, server systems, and network components including routers, firewalls, or any other DoIT IT asset. Assessments shall also include any critical web-based applications. All tests will be performed on production and test systems.

External and internal security assessments by third party security services shall be performed annually.

Where regulatory requirements require more specific or different vulnerability identification response processes and procedures, then the regulatory requirement will be followed for systems and applications subject to the regulatory requirement.

Assessments at a minimum should include port scanning, unneeded services, patch level assessment, active exploits, weak passwords, misconfiguration, and rogue wireless access points [Known vulnerabilities as listed in Common Vulnerabilities and Exposures (CVE) (http://cve.mitre.org)]. The Network Security Team will use SANS and other security organizations 'Top 20' vulnerabilities list as a guide to determine specific items to test, and OWASP Top 10 to test web applications.

The objectives of a Vulnerability Assessment and related processes include:

a. Discovering internal and external system risks

b. Creating a mitigation plan of action with milestones for any risks which are discovered

c. Maintaining a pro-active approach to IT security; and

d. Ensuring all IT systems employ best security practices and DoIT I.S. Policies.

5.2 Penetration Testing

Internal and external penetration testing shall be done annually and after any significant changes tothe environment. Penetration testing will be based on industry-accepted penetration testing approaches, such as NIST SP800-115. Testing must occur from both inside and outside the network, validate any segmentation, if used, and include application layer and network layer testing. Detailed assessment reports must include outlining of all tools, tests, and methods used to conduct the test. Assessment reports must include all findings and recommendations for mitigating vulnerabilities discovered. Corrective measures are to follow appropriate change management processes.

Documentation of assessments and penetration tests must be kept for at least 24 months.

NMAC 1.12.20.24 PENETRATION AND INTRUSION TESTING

A. Penetration analysis and testing shall be used to determine whether:
1) a user can make an unauthorized change to an application;
2) a user can access the application and cause it to perform unauthorized tasks;
3) an unauthorized individual can access, destroy or change any data;
4) an unauthorized individual may access the application and cause it to take actions unintended by the application designer(s).

B. The output of the penetration testing and intrusion testing shall be reviewed by the agency ISO and any vulnerability detected shall be evaluated for risk and steps taken to mitigate the risk.

C. Any tools used to perform the penetration testing shall be kept updated to ensure that recently discovered vulnerabilities are included in any future testing.

D. Where an agency has outsourced a server, application, or network services to another agency, independent penetration testing shall be coordinated by both agencies.

E. Only an individual or individuals authorized in writing by the agency shall perform penetration testing. The agency ISO shall notify DoIT security staff two business days prior to any penetration test. Any attempt by the agency to perform penetration testing without prior notice to DoIT shall be deemed an unauthorized access attack which shall be reported to the state CIO.

F. All documents pertaining to security penetration tests, security investigations, security data and reports shall be categorized as sensitive and protected from public disclosure. Counsel for the agency shall review and approve such information to ensure compliance with state law.

6. CONFIDENTIALITY

All documents pertaining to risk assessments, vulnerability scanning, security penetration tests, security investigations, security data and reports shall be categorized as sensitive and protected from public disclosure, including but not limited to requests for information pursuant to the Inspection of Public Records Act. DoIT's General Counsel shall review and approve such information to ensure compliance with state law.

7. ROLES AND RESPONSIBILITIES

a. DoIT CISO

The DoIT Chief Information Security Officer (CISO) or Chief Information Officer (CIO) designee is responsible for the implementation and maintenance of the Vulnerability Management and Assessment Policy and program. The CISO or CIO designee shall approve in writing any of the assessments prior to them being initiated. All assessments must be scheduled and documented. The assessment reports will be stored and held by the CISO or CIO designee. The CISO or CIO designee is responsible for recommending mitigation strategies and ensuring system administrators resolve any risks that are discovered.

b. DoIT Network Security Team

The DoIT Network Security Team is responsible for monitoring security vulnerability alerts fortheir assigned technology support areas. This includes technical and support employees responsible for DoIT systems and technologies, such as Microsoft server administrators, database administrators, network and router support personnel, application support, etc.

The DoIT Network Security Team will subscribe to intelligence threat feeds, patch notifications, and security feeds to maintain knowledge of current threat landscapes. Upon receiving an alert, staff will analyze the alert to determine if it affects DoIT systems, the potential risk and impact to our systems, and options or steps, if any, for mitigating vulnerability, such as patching, blocking ports, or other steps. Internal vulnerability scan processing and reporting must be reviewed within 24 hours of receipt. Any found vulnerability must be analyzed and an action plan developed for risk mitigation where applicable.

8. EXCEPTIONS

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

9. 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.

10. REFERENCES

a. Payment Card Industry Data Security Standards v3.2: Requirements 5 and 6, 11.3
b. National Institute of Standards and Technology SP800-53 r4: RA-5, CA-5, CA-8, SA-11
c. International Organization for Standardization/International Electrotechnical Commission 27002:2013: 12.6, 18.2.3
d. Controls Objectives for Information and Related Technologies v5.0
e. National Institute of Standards and Technology SP800-115 Technical Guide toInformation Security Testing and Assessment
f. SANS 'Top 20' vulnerabilities (https://www.sans.org/critical-security-controls/)
g. Common Vulnerabilities and Exposures (CVE) (http://cve.mitre.org)
h. OWASP Top 10 for web applications (https://www.owasp.org)

11. 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
06/23/2021	4	Olga Serafimova	Reviewed and revised for legal compliance
05/20/2022	5	Brenda Fresquez	Reviewed for quality assurance

Approval

DocuSigned by:
437214FBE82C453...

6/15/2022

Raja Sambandam, Acting Cabinet Secretary **Date**