NM DEPARTMENT OF INFORMATION TECHNOLOGY

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

| | |
|---|---|
| **Policy Title:** | **Information Risk Assessment Policy** |
| **Policy Number:** | **DoIT-361-709** |
| **Effective Date:** | **3/21/22** |
| **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 (such as through the world-wide web), shall be subject to annual independent penetration analysis and intrusion testing by qualified, independent third-party contractor approved by DoIT.

## 2. PURPOSE

This Policy establishes security risk assessment requirements for information technology (IT) telecommunications, computing,networks, storage, data, and applications. Security risk assessments provide a mechanism to identifysecurity requirements by identifying threats, vulnerabilities, and security and control issues. Security risk assessments also provide a basis to compare cost of risk to cost of mitigation.

## 3. SCOPE

This policy applies to DoIT telecommunications, computing, networks, storage, data, applications, and employees.

## 4. DEFINITIONS

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

b. **Risk Assessment –** Identifying and analyzing potential events that may negatively affect theState and providing a remediation decision based on the acceptable amount of associated risk from the analysis.

c. **Risk –** The likelihood of a given threat source exploiting a particular potential vulnerability, and the resulting impact of that adverse event on the organization.

d. **Vulnerability –** A weakness that allows an attacker to violate the integrity or to reduce the information assurance of an IT asset. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.

e. **Vulnerability Scanning** – A security technique used to identify security weaknesses in an IT asset. Vulnerability scanning is performed using industry-standard automated software toolsdesigned to assess computers, computer systems, networks, or applications for weaknesses.

## 5. POLICY

DoIT will perform IT Risk Assessments at least annually and whenever there is a significant change in systems or IT environment. By identifying risks proactively, DoIT can manage and mitigate risks effectively. Risk Assessments will take into consideration security and compliance standards such as Payment Card Industry Data Security Standard (PCI DSS), Internal Revenue Service (IRS) Publication 1075, Health Insurance Portability and Accountability Act (HIPAA), and Fair Credit and Reporting Act (FCRA). Identified Risks will be categorized based on the significance of the Risk to the State of New Mexico. DoIT or DoIT-contracted staff shall assess risks using qualitative or quantitative analysis, security assessment, Vulnerability Scanning, penetration testing, tabletop exercises and other evaluation criteria as deemed appropriate.

The DoIT Chief Information Security Officer (CISO) or Chief Information Officer (CIO) designee will prioritize identified risks and will ensure development and implementation of mitigation plans addressing, at a minimum, high-risk items.

**Penetration analysis and testing shall be used to determine whether:**

a. a user can make an unauthorized change to an application;
b. a user can access the application and cause it to perform unauthorized tasks;
c. an unauthorized individual can access, destroy, or change any data; and
d. an unauthorized individual may access the application and cause it to take actions unintended by the application designer(s).

The output of the penetration testing and intrusion testing shall be reviewed by DoIT's CISO or CIO designee and any vulnerability detected shall be evaluated for risk and steps taken to mitigate the risk.

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

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

## 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 CISO or CIO designee willensure development, documentation, updates, and distribution of information as necessaryto ensure the Risk Assessment process is known and executed. The CISO or CIO designee will identify and implement Risk Assessment tools and will document compliance requirements.

### b. DoIT Staff

Only an individual or individuals authorized in writing by the CISO, the CIO, or CIO designee shall perform penetration testing. All DoIT staff are responsible for following the procedures to conduct Risk Assessments.

## 8. EXCEPTIONS

The DoIT CIO or DoIT 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. 1.12.20.24 NMAC
b. Payment Card Industry Data Security Standards v3.2: 12.2
c. National Institute of Standards and Technology 800-37 Rev.1, Guide for Applying the Risk Management Framework to Federal Information Systems
d. National Institute of Standards and Technology 800-30 Rev.1, Guide for Conducting Risk Assessments
e. National Institute of Standards and Technology 800-53 Rev. 4, Recommended SecurityControls for Federal Information Systems: CA-2, CA-2(1), RA-1, RA-2, RA-3, RA-5
f. National Institute of Standards and Technology 800-161, Supply Chain Risk Management Practices Federal Information Systems and Organizations
g. International Organization for Standardization/International Electrotechnical Commission 27002:2013: 8.2.1, 12.6.1, 14.2.2
h. Information Systems Audit and Control Associations Controls Objectives for Information and Related Technologies v5.0
i. New Mexico Statutes Annotated (NMSA) Chapter 9
j. Department of Information Technology Vendor Management Policy

## 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 |
| 06/03/2021 | 4 | Olga Serafimova | Reviewed and revised for legal compliance |
| 12/28/2021 | 5 | Brenda Fresquez | Reviewed for quality assurance |
| 3/15/2022 | 6 | Marko Satarain | No changes, reviewed and accepted by HR—Marko Satarain, Legal—Todd Baran and CWA—Dan Secrist |

### Approval

DocuSigned by:
437214FBE82C453...

3/21/2022

**Raja Sambandam, Acting Cabinet Secretary**

**Date**