

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

Policy Title:	Security Awareness Training Policy
Policy Number:	DoIT-361-715
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 1.12.20.27(H) NMAC, DoIT must provide training to all DoIT IT Resource Users to raise their awareness with respect to risks resulting from the use of such resources and what controls are in place to protect State data and equipment.

2. PURPOSE

This Policy establishes requirements for mandatory security awareness training for all DoIT IT Resource Users to be conducted when initially joining DoIT and annually thereafter.

3. SCOPE

This policy applies to all DoIT IT Resource Users.

4. DEFINITIONS

- a. **DoIT IT Resource Users** - All DoIT employees, contractors, vendors, consultants, temporary staff, seasonal staff, and any other users of DoIT IT resources.
- b. **Information Technology Resources (IT resources)** means computer hardware, software, databases, electronic message systems, communication equipment, computer networks, telecommunications circuits, and any information used by a State agency to support programs or operations that is generated by, transmitted within, or stored on any electronic media.
- c. **Phishing** - the fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal confidential or personal information, such as passwords or credit card numbers.
- d. **Social Engineering** - the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.
- e. **Spoofing** - when an untrusted source attempts to impersonate communications from a known trusted source to gain access to attempt a larger cyber-related attack (for example, phishing, social engineering, man-in-the-middle, etc.).



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

5. POLICY

The security, confidentiality, integrity, and availability of data owned or maintained by DoIT is critical to State operations. All DoIT IT Resource Users must complete a security and privacy awareness training that promotes a basic understanding of the need for information security, potential threats (internal or external) against the State, and of user actions necessary to maintain security and to respond to suspected security related incidents. DoIT may employ additional security and privacy awareness training techniques such as displaying relevant posters, disseminating email advisories, displaying logon screen messages, or conducting information security awareness events.

DoIT may test employee security and privacy awareness unannounced and at any time and must do so at least annually. Testing may include email phishing, phone spoofing, requests bypassing critical policies or procedures, or other forms of simulated attack.

6. ROLES AND RESPONSIBILITIES

a. DoIT CISO

The DoIT Chief Information Security Officer (CISO) or Chief Information Officer (CIO) designee is responsible for ensuring a security awareness program - and an associated training - is designed, delivered, and managed to ensure all DoIT IT Resource Users are aware of security risks, best practices, and conduct requirements.

The CISO must ensure training is maintained and evolves with the changing security landscape. Employee training attendance must be audited at least every 60 days to ensure no training gaps occur and that all DoIT IT Resource Users comply.

b. DoIT Management

DoIT managers and supervisors are responsible for ensuring their direct reports attend the security awareness training within the first 30 calendar days of hire and at least annually thereafter.

c. DoIT Information Security Staff

DoIT Security Staff are any staff assigned by DoIT CISO or DoIT CIO. Security Staff are responsible for ensuring further security education and training by joining cybersecurity industry accredited security groups and associations to manage current and future threat-landscapes.

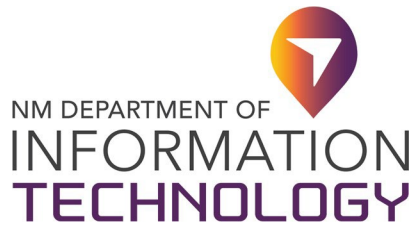
d. DoIT IT Resource Users

DoIT IT Resource Users are responsible for attending all mandatory security awareness trainings, successfully completing within the required timeframes, and maintaining their annual security awareness training certification.

7. EXCEPTIONS

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

8. VIOLATIONS OF POLICY



Michelle Lujan Grisham

New Mexico Governor

Raja Sambandam

Acting Cabinet Secretary & State CIO

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

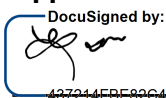
9. REFERENCES

- a. 1.12.20 NMAC
- b. SysAdmin, Audit, Network and Security Institute: Security Awareness Training and Privacy
- c. National Institute of Standards and Technology: 800-50, Building an Information Technology Security and Awareness Training Program
- d. National Institute of Standards and Technology SP800-53 r4: AR-5, AT-2(2), PM-15

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
05/21/2021	4	Olga Serafimova	Reviewed and revised for legal compliance.
5/10/2022	5	Brenda Fresquez	Reviewed for quality assurance

Approval

DocuSigned by:

 407214FBE82C453...

Raja Sambandam, Acting Cabinet Secretary

6/15/2022

Date