NM DEPARTMENT OF INFORMATION TECHNOLOGY

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

Policy Title:	**Information Security Policy**
Policy Number:	**DoIT-361-700**
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 the Department is charged.

Per 1.12.20.16 NMAC, to maintain information security, DoIT must require through published policies and procedures consistent with 1.12.20 NMAC, that individual accountability be maintained at all times, including during remote access.

2. PURPOSE

DoIT considers its information assets, including customer information ("Information Assets"), to besignificant and valuable resources. This Information Security Policy (this "I.S. Policy"), together with its attendant security policies, below, provide direction and rules necessary to protect Information Assets from threats or hazards, whether internal or external, deliberate, or accidental. The objective of this I.S. Policy is to limit the risks to Information Assets that might compromise DoIT's operations through the loss of information confidentiality, integrity, reliability, or availability.

3. SCOPE

This I.S. Policy applies to all DoIT IT Users and others who may haveaccess to DoIT Information Assets and systems.

4. DEFINITIONS

a. **.gov** –The ".gov" domain hosts only official government sites at the federal, state, and local government levels. The ".gov" domain provides the official and trusted Internet presence for these government entities.
b. **Access Control Badge** - An identification badge that enables programmable access to secure entrances.
c. **Access Control Reader** - A device that controls access and detects authorized personnel moving in and out of secure areas by reading an Access Control Badge and permitting or denyingentrance based on privilege.
d. **Access Control System** - An automated system that manages personnel access to secure locations and has the ability to lock, unlock, track, and record door access, and to alert monitoring staff as to personnel's ingress and egress throughout facilities.

e. **Access-Control List (ACL)** – A table of acceptable users, groups, or IP addresses that are provided access to the information system or network.
f. **Advanced Encryption Standard (AES-CCM)** – A wireless encryption protocol specified by the Institute of Electrical and Electronics Engineers (IEEE) 802.11i. It is currently regarded as the strongest form of wireless encryption.
g. **Anti-Malware/Virus Software** – Software designed to detect, contain, or otherwise eradicate malicious code.
h. **Apps –** Applications installed on a mobile device.
i. **Authorized User –** Any user who has DoIT's permission to use a State- issued mobile device.
j. **Change Control Board (CCB) -** The body that authorizes changes and assists in assessing and prioritizing changes.
k. **Change Initiator -** Party who generates the initial request for a production change.
l. **Change Owner -** Party responsible for post-review change execution and advisement of how to communicate change procedures, lead change reviews for their appropriate service area, and perform change postmortems.
m. **Computer Security Incident -** Any network or host activity that potentially threatens the security of computer systems; any real or suspected adverse event in relation to the security of computer systems or computer networks.
n. **Confidential Data –**Data which, if compromised in some form or fashion, is likely to result in significant and/or long-term harm to the institution and/or individuals whose data it is.
o. **Contractor -** A person or company that undertakes a contract to provide materials or labor to perform a service to do a job.
p. **Counter with Cipher Block Chaining Message Authentication Code (CBC-MAC) –** Technique for creating a message authentication code from a block cipher.
q. **Custodian** - A third-party entity that holds and safeguards a user's private keys or digital assets on their behalf. Depending on the system, a custodian may act as an exchange and provide additional services, such as staking, lending, account recovery, or security features.
r. **Data Breach Incident –** Any event resulting in compromise of DoIT or DoIT customer data, including but not limited to unauthorized release, loss, or theft; unauthorized access or use; and/or misplacement, public display, or verbalization, wherein such event results in substantial harm or inconvenience to DoIT or the DoIT customer(s).
s. **Data Classification –** A method of defining and categorizing data to determine type, protection requirements, access level, and labeling.
t. **Data Management Zone or DMZ –** A physical or logical sub-network that contains and exposes DoIT's external services to a larger untrusted network, typically the Internet.
u. **DoIT IT Resource Users -** All DoIT employees, contractors, and any other users of DoIT IT resources.
v. **Domain –** A region of jurisdiction on the Internet for naming assignment.
w. **Domain Name –** A name assigned to an Internet server that locates an organization or entity on the Internet.
x. **Domain Name System (DNS) –** DNS is a hierarchal distributed naming system for computers, Services, or any resources connected to the Internet or to a private network.
y. **Emergency Change -** A change request used only when a change must be performed immediately to resolve a critical condition.
z. **Extensible Authentication Protocol (EAP) –** A series of authentication methods used inside 802.1x to achieve wireless authentication.
aa. **Federal Risk and Authorization Management Program (FedRAMP) –** A US government-wide program that provides standardized approach to security assessments, authorization, and continuous monitoring for cloud products and services.
bb. **Federal Taxpayer Information –** Information used by the Internal Revenue Service to

identify taxpayers personal and business tax return data.

cc. Firewall – Security systems that control and restrict network connectivity and network services per a pre-defined policy and rule set.

dd. Floater Devices – Devices that are not assigned to a specific person but are used by multiple individuals.

ee. Hardening – Configuring a system to minimize the opportunity for compromise.

ff. Information Owners - Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

gg. Internet Protocol Security (IPSEC) – An Internet Engineering Task Force (IETF) standard for protecting IP communication by encrypting or authenticating all packets.

hh. Intrusion Detection System – Device or software application that monitors an information system for malicious activity or policy violations.

ii. Intrusion Prevention System – Network security system that detects and prevents identified cyber threats.

jj. Jail Broken or Rooting – Altering a mobile device's operating system to remove or circumvent restrictions.

kk. Malware – Software designed to interfere with a device's normal operating function.

ll. Media Access Control (MAC) – A unique identifier assigned to a network interface controller (NIC) as a network address when communicating with a network segment.

mm. Messages – Include, but are not limited to, Short Message Services (SMS), emails, Multimedia Message Services (MMS), Blackberry Messenger (BBM), iMessage's, and services provided through social media sites.

nn. Namespace – A container for a set of identities that provides a level of indirection to specific identifiers while retaining a global uniqueness.

oo. Non-production Network – Any network used solely for testing, development, training, or other non-production purposes.

pp. NT File System (NTFS) – A proprietary journaling file system developed by Microsoft, which is the default file management system of the Windows NT family.

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

rr. Payment Card Industry Data Security Standard (PCI DSS) – An information security standard for the protection and handling of branded credit card information to help organizationsproactively protect customer account data.

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

tt. Personal Devices – User devices that have not been provided by DoIT.

uu. Personally Identifiable Information (PII) - Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual incontext.

vv. Phishing - The fraudulent practice of sending Messages purporting to be from reputable sources to induce recipients to reveal personal information, such as passwords orcredit card numbers.

ww. Physical Security Staff - Physical security officers and manager.

xx. Privacy Incident - Only those incidents relating to Personally Identifiable Information (PII).

yy. Production Network – The network used for DoIT's daily business, whose impairment would result in direct loss of functionality for DoIT IT Resource Users and/or customers; any network connected to a DoIT backbone, either directly or indirectly, which lacks an interveningfirewall device; or any network whose impairment would result in direct loss

of functionality for DoIT IT Resource Users or customers.

zz. Production or Production Environment - Active network, servers, storage, Telecommunications, and/or applications that operate to serve DoIT's day-to-day operations.

aaa. Public Data – Data that may be freely disclosed without restriction.

bbb. Remote Access – Any access to DoIT's network through a non-DoIT-controlled network, device, or medium.

ccc. Removable Media – Storage devices designed to be inserted and removed from information systems and workstations, such as USB drives, CD/DVD-ROM drives, portablehard drives, etc.

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

eee. Risk Assessment – Identifying and analyzing potential events that may negatively affect the State, and providing a decision based on the acceptable amount of associated risk from the analysis.

fff. Router - A device that forwards data packets along networks based on configured routes and ACL.

ggg. Secure Shell (SSH) – Cryptographic network protocol for operating network services securely over an unsecured network.

hhh. Secure Socket Layer/Transport Security Layer (SSL/TLS) – Encryption protocols used to protect the transfer of data and information within an IP network.

iii. Secured Areas - Any area with access restricted by Access Control Readers.

jjj. Security Access Application - A form used to request access to DoIT facilities.

kkk. Sensitive Data – Data which, when released without authorization, could be expected to cause minor or short-term harm to the institution or individuals whose data it is and is intended only for limited dissemination.

lll. Server – An internal DoIT Server hosting client, DoIT services, or applications.

mmm. Service and Organization Control 2 (SOC2) – A report on various organizational controls related to security, availability, processing integrity, confidentiality, or privacy.

nnn. Service Set Identifiers (SSIDs) – An IEEE 802.11 wireless networking naming standard used to differentiate multiple wireless networks that overlap with each other.

ooo. Simple Network Management Protocols – A protocol for collecting and organizing information about a managed device on IP networks.

ppp. Social Engineering - the use of deception to manipulate individuals into divulging confidential, sensitive, or personal information that may be used for fraudulent purposes.

qqq. Spoofed Webpage – A website created as a hoax with the intention of misleading visitors to believe the website was created by a different person or organization.

rrr. Spoofing – when an untrusted source attempts to impersonate communications from known trusted source to gain access or to attempt a larger cyber-related attack.

sss. Switch – A device that filters and forwards packets between LAN segments.

ttt. Tailgating - Also known as "Piggybacking", the practice of intentionally or unintentionally following an Authorized User to gain access to an Secured Area without using an Access Control Badge.

uuu. Temporary Access Control Badge - A Day access badge worn by a DoIT employee who has forgotten, lost, or misplaced their Access Control Badge.

vvv. Test Network – A network used for the purposes of testing, demonstration, and training to prevent a disruption in the Production environment.

www. Transmission Control Protocol Wrapper (TCP Wrapper) – Host-based networking ACL system used to filter network access to IP servers on an operating system.

xxx. Uniform Resource Locator (URL) - A specific character string that constitutes a reference

to a specific resource.

yyy. Update – An act of bringing something up to date, or an updated version of something; to make something more modern or current.

zzz. User Acceptance Testing – The act of verifying that a software update is functional and working as desired for application or system use.

aaaa. Vendor – a supplier, individual, or company that provides goods or services to DoIT.

bbbb. Virtual Private Network (VPN) – An encrypted network that extends a private network across a public network to allow a user to send and receive data as if their computing device wereconnected to the private network.

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

dddd. Visitor - An individual who DoIT security has signed in to a DoIT facility, and who must be escorted and sponsored by DoIT staff.

eeee. Voice Over IP (VoIP) – A protocol for telecommunications over IP based networks.

ffff. Vulnerability – A weakness that allows an attacker to violate the integrity or to reduce the information assurance of an IT asset.

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

hhhh. Vulnerability Scanning – A security technique used to identify security weaknesses in an IT asset.

iiii. Wi-Fi Protected Access Version 2 (WPA2) – WPA2 implements the full IEEE 802.11i standard but will not work with some legacy network cards. Products displaying the WPA2 logo havepassed a certification program run by the Wi-Fi Alliance

5. POLICY

DoIT's Information Security Program represents the set of policies and controls necessary to maintain a secure information services provider environment. Information security documentation ("Documentation") and policies must be readily available for DoIT's internal review, and DoIT willreview and update these policies and information security documentation at least annually. The Information Security Program is designed to ensure that information is protected against unauthorized access, that confidentiality of information is assured, that integrity of information is maintained, and that regulatory and legislative requirements are met where applicable. The Information Security Program also ensures that all staff are trained on information security and that disaster recovery plans are produced, maintained, and tested.

The DoIT Chief Information Security Officer (CISO) is responsible for ensuring that specific Information Security Policies and Information Security Procedures are developed to support thisgeneral DoIT Policy. These include the following policies:

a. ACCEPTABLE USE OF IT RESOURCES POLICY
b. ANTI-MALWARE/VIRUS POLICY
c. IT CHANGE MANAGEMENT POLICY
d. DATA CLASSIFICATION POLICY

- **e.** DOMAIN NAME MANAGEMENT POLICY
- **f.** FIREWALL POLICY
- **g.** INCIDENT RESPONSE POLICY
- **h.** INFORMATION SYSTEMS LOGGING AND MONITORING POLICY
- **i.** IT RISK ASSESSMENT POLICY
- **j.** ENTERPRISE MOBILE DEVICE SECURITY AND USAGE POLICY
- **k.** NETWORK DEVICE CONFIGURATION POLICY
- **l.** PATCHING AND UPDATING POLICY
- **m.** PHYSICAL ACCESS POLICY
- **n.** REMOTE NETWORK ACCESS POLICY
- **o.** SECURITY AWARENESS TRAINING POLICY
- **p.** SYSTEMS CONFIGURATION POLICY
- **q.** VENDOR MANAGEMENT POLICY
- **r.** VULNERABILITY MANAGEMENT AND ASSESSMENT POLICY
- **s.** WIRELESS SECURITY POLICY

6. ROLES AND RESPONSIBILITIES

a. DoIT CISO

The DoIT CISO, working on behalf of the Secretary ofDoIT/ State Chief Information Officer (CIO), or a CIO designee, is responsible for planning, managing, and overseeing execution of the Information Security Program and policies for DoIT.

b. Information Owners

Information owners designate the relevant sensitivity classification for each type of information contained in/used by each application, in accordance with the *Data Classification Policy*. Information owners also designate the level of criticality, identify which users will be granted access to a given application, and approve or disapprove requests for ways in which the information will be used. Information owners must take steps to ensure that appropriate controls are used in storing, handling, distributing, and using information.

c. Custodians

Custodians are responsible for safeguarding information in any application for which they aredesignated responsibility. This includes implementing Access Control Systems to prevent inappropriate disclosure of information and backing up data to ensure that critical information is not lost. Custodians must implement, operate, and maintain security measures defined by information owners.

d. DoIT IT Resource Users

DoIT IT Resource Users are required to familiarize themselves with and to comply with all DoIT Information Security policies, procedures, and standards. Each employee must adhere to Information Security policies and/or applicable procedures. All users of DoIT information must comply with control requirements specified by the information owner and/or the custodian(s).

Users must:

- **i.** Be personally aware of procedures, risks, and protective measures related to any system or information that they are using.
- **ii.** Obtain proper authorization to access information.
- **iii.** Understand that being granted access to information does not imply or confer authority to (i) grant

other users access to that information; (ii) share that information in any way with individuals who have not been granted access; or (iii) use information for any purpose that is not directly related to the user's work responsibility.

iv. Comply with relevant laws, regulations, and rules regarding information access andthe operation of protective measures.

v. Report to their supervisor any issues, circumstances, or weaknesses insecurity arrangements.

vi. Direct questions about the appropriate handling of a specific type of information to either the Custodian or the Owner of the involved information.

e. DoIT Managers

DoIT managers (i.e., executive staff, division directors, bureau chiefs, managers, supervisorsand team-leads) are directly responsible for implementing the I.S. Policies and procedures within their respective work areas and for adherence by their staff.

DoIT managers must ensure system and data owners are identified, appointed, and made of their responsibilities. DoIT managers also have an advisory and assisting role to IT and non-IT managers to help identify and assess risks, to identify and implement protective measures (including compliance with these practices), and to maintain a satisfactory level ofsecurity awareness. DoIT managers must monitor the proper operation of security measures within their teams, investigate weaknesses and incidents, and raise any new issues or circumstances of which they become aware through their roles.

f. DoIT Network Security Administrators

DoIT Network Security Administrators who provide security administration of user IDs, permissions, and access rights or who provide technical security administration are responsible for implementing Information Security policies and for implementation of information security for their areas of responsibility. Network Security Administrators follow security procedures and practices for assigned applications or platforms; ensure that accurate, up-to-date records are kept of authorized and unauthorized access attempts; and monitor the applicability and effectiveness of DoIT Information Security policies, practices, and procedures.

7. EXCEPTIONS

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

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. National Institute of Standards and Technology: SP800-41

b. Sysadmin, Audit, Network and Security Institute: Information Security Policies andProcedures

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 Sambandam	Revised and routed for Union approval

06/23/2021	4	Olga Serafimova	Reviewed and revised for legal compliance
12/28/2021	5	Brenda Fresquez	Reviewed for quality assurance
11/13/2023	5.1	Brenda Fresquez	Annual Review: updated header and footer
11/13/2023	5.1	Bryan E. Brock	Annual Review - Legal. No changes recommended.

Approval

DocuSigned by:
437214FBE82C453...

11/14/2023

Raja Sambandam, Acting Cabinet Secretary **Date**