NM DEPARTMENT OF
INFORMATION
TECHNOLOGY

Michelle Lujan Grisham
New Mexico Governor

Raja Sambandam
Acting Cabinet Secretary & State CIO

Policy Title:	**Wireless Security Policy**
Policy Number:	**DoIT-361-719**
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 1.12.20.19 NMAC, specific security precautions must be implemented prior to installing any wireless networks or wireless access points.

2. PURPOSE

This Policy provides employees and other users of DoIT systems direction on the proper use and protection of DoIT's internal network by establishing standards for wireless technology usage. ThisPolicy prohibits any access to DoIT networks via an unsecured wireless communication medium.

Only wireless devices meeting the criteria of this Policy may be approved for connectivity to DoIT's networks.

3. SCOPE

This Policy applies to all DoIT IT Resource Users connecting to DoIT networks using any wireless data communication devices. Wireless devices include DoIT-owned computers, cellular phones, tablets, and any other devices that connect to DoIT's internal or Guest/Internet networks through wireless technologies. Any device not owned and managed by DoITwill be connected to the Guest/Internet access only wireless networks.

4. DEFINITIONS

a. **Advanced Encryption Standard (AES-CCM)** – A wireless encryption protocol specified by the Institute of Electrical and Electronics Engineers (IEEE) 802.11i; currently regarded as thestrongest form of wireless encryption.

b. **Counter with Cipher Block Chaining Message Authentication Code (CBC-MAC)** – Techniquefor creating a message authentication code from a block cipher.

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

d. **Extensible Authentication Protocol (EAP)** – A series of authentication methods used inside802.1x to achieve wireless authentication.

- **e.** **Internet Protocol Security (IPSEC)** – An Internet Engineering Task Force (IETF) standard for protecting IP communication by encrypting or authenticating all packets.
- **f.** **Service Set Identifiers (SSIDs)** – An IEEE 802.11 wireless networking naming standard used to differentiate multiple wireless networks that overlap with each other.
- **g.** **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 were connected to the private network.
- **h.** **Wi-Fi Protected Access Version 2 (WPA2)** – WPA2 implements the full IEEE 802.11i standardbut will not work with some legacy network cards. Products displaying the WPA2 logo have passed a certification program run by the Wi-Fi Alliance.

5. POLICY

At its facilities, DoIT provides wireless network capabilities for connecting to the DoIT internal network. Only approved and securely configured access points are permitted on this network. Access points provide separate Service Set Identifiers (SSIDs) and networks for Guest/Internet-only access and for corporate network connectivity. DoIT staff monitor network traffic and connections granted to users and devices connected to DoIT wireless networks.

DoIT maintains a list of all DoIT maintained wireless Local Area Networks (LANs) and maintains security controls around the wireless environments. DoIT maintains up-to-date network diagramsthat show all communication links, including LAN, Wireless Area Network (WAN), and Internet.

Event logging on wireless networks is offloaded or copied to a secure centralized log server or media. Rogue access point detection is conducted on a quarterly basis, and any rogue access points detected on the DoIT network are required to be mitigated according to the Incident Response Plan.

5.1. Wireless Device Monitoring

DoIT is responsible for deploying mechanisms that monitor Wi-Fi connections. Any rogue wireless networks are analyzed to determine if they impact DoIT operations or create a security incident. Testing for the presence of any unauthorized wireless access points is conducted at least on a quarterly basis. DoIT uses wireless intrusion detection systems that are incorporated into the wireless LAN access whenever possible.

5.2. Wireless Authentication

All wireless networks are required to have methods of authenticating users. Passwords for all access points must adhere to the Password Policy as defined in **NMAC 1.12.11.16 SECURITY.** DoIT only uses the highest level of encryption, such as WPA2 with 802.1x/Extensible Authentication Protocol-Protected Extensible Authentication Protocol (EAP-PEAP). Where 802.1x authentication is used, mutual authentication must be performed. All DoIT IT Resource User devices must validate digital certificates by the authentication server and must be trusted and valid. DoIT IT Resource Users may not disable validation of server certificates and blindly trust any certificate presented. EAP methods that do not support certificate-based mutual authentication may not be used. Legacy devices not capable of WPA2 must be isolated and restricted to the minimum required wireless network access.

5.3. Wireless Encryption

All wireless communication must be encrypted between DoIT devices and networks. Wireless networks providing Internet access only for guests are exempt from this requirement. DoIT uses onlyWPA2 using AES-CCM encryption. Any device not capable of supporting WPA2 must be secured usingVPN technology such as IPSEC.

5.4. DoIT IT Resource User Security Standards

Where supported by the DoIT IT Resource User operating system and wireless system, the wireless network performs checks for minimum-security standards prior to granting access to a DoIT network. Any device connecting to a DoIT network is required to use DoIT approved anti-virus software with current definitions. All wireless devices must have updated vendor patches/firmware for all software on the device. Any DoIT IT Resource User device that does not support DoIT integrity checking will be given, at most, restricted access to the DoIT network in accordance with specific business requirements.

5.5. Wireless Guest Access

By default, all users not employed by DoIT, or wireless users who have equipment that is not ownedand managed by DoIT, will receive access only to the Guest/Internet-only wireless networks.

All wireless guest access must be authenticated through a web-based authentication system. Logon credentials with username/password combination must be assigned for each guest account. DoIT staff review guest account access monthly to verify active accounts and to disable inactive accounts.Wireless guest access will be granted for use only during normal business hours. If access is requiredoutside of normal business hours, a designated DoIT manager must approve the request before access is granted. Each guest account is restricted to using only 2 Megabytes per user and must only have access to the following protocols:

a. Hyper Text Transfer Protocol (HTTP) (TCP port 80)

b. Hyper Text Transfer Protocol Secure (HTTPS) (TCP port 443)

c. Post Office Protocol (POP3) (TCP port 110)

d. Internet Key Exchange (IKE)(UDP port 500)

e. Internet Protocol Security (IPSEC) Encapsulating Security Payload (ESP) (IP protocol 50)

f. Point-to-Point Tunneling Protocol (PPTP) (TCP port 1723)

g. Generic Routing Encapsulation (GRE) (IP protocol 47)

h. Dynamic Host Control Protocol (DHCP) (UDP ports 67-68)

i. Domain Name System (DNS) (UDP port 53)

j. Internet Control Message Protocol (ICMP) (IP protocol 1)

NMAC 1.12.20.19 WIRELESS NETWORKS, BLUETOOTH, AND RADIO FREQUENCY IDENTIFICATION:

A. No **wireless** network or **wireless** access point shall be installed prior to an agency performed risk assessment and the written approval of the agency CIO.

B. Suitable controls, such as media access control (MAC), address restriction, authentication, and encryption, shall be implemented by the agency to ensure that a **wireless** network or access point cannot be exploited to disrupt agency information services or to gain unauthorized access to agency information. When selecting **wireless** technologies, such as 802.11x or its predecessors or its successor, **wireless** network security features on the equipment shall be available and implemented at the time of deployment.

C. Access to systems that hold sensitive information or the transmission of protected or sensitive information via a **wireless** network is not permitted unless and until appropriate and adequate measures have been implemented and approved by the state CIO. Such measures shall include authentication, authorization, encryption, access controls, and logging.

6. ROLES AND RESPONSIBILITIES

a. DoIT CISO

The DoIT Chief Information Security Officer (CISO) or Chief Information Officer (CIO) designee is responsible for overall compliance with this Policy. The CISO or CIO designee also reviews and signs off on quarterly rogue access point reports beforethey are formally stored for audit.

b. Network Security Team

The Network Security Team (NST) is responsible for maintaining wireless networks in accordance with this Policy. The NST maintains documentation (e.g., list, diagrams) of all active wireless networks, performs quarterly rogue access point detection, and ensures the highest level of encryption and authentication is used on Wi-Fi networks when technically possible.

c. DoIT IT Resources Users

DoIT IT Resource Users are responsible for adhering to this Policy and may not create,modify, or join unapproved wireless networks within DoIT's infrastructure.

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 andincluding termination of employment.

9. REFERENCES

- **a.** National Institute of Standards and Technology SP800-53 r4: AC-18(1)
- **b.** International Organization for Standardization/International Electrotechnical 27002:2013:13.1.1, 13.1.3, 9.1.2
- **c.** National Institute of Standards and Technology SP800-153, Guidelines for Securing WirelessLocal Area Networks (WLANs)

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
06/23/2021	4	Olga Serafimova	Reviewed and revised for legal compliance
5/26/2022	5	Brenda Fresquez	Reviewed for quality assurance

Approval

DocuSigned by:
437214FBE82C453...

6/15/2022

Raja Sambandam, Acting Cabinet Secretary

Date