NM DEPARTMENT OF INFORMATION TECHNOLOGY

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

Policy Title:	**Remote Network Access Policy**
Policy Number:	**DoIT-361-714**
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 1.12.20.16 NMAC, each agency is required to have published policies addressing remote access individual accountability.

2. PURPOSE

This Policy establishes minimum security requirements for remote access to DoIT's network and computer systems. This Policy provides direction to mobile or remote users to ensure DoIT information and computer-related assets are protected.

3. SCOPE

This Policy applies to all DoIT IT Resource Users who remotely connect to the DoIT network and resources.

4. DEFINITIONS

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

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

c. **Secure Shell (SSH) –** Cryptographic network protocol for operating network servicessecurely over an unsecured network.

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

e. **Virtual Private Network (VPN) –** A network that uses a public telecommunication infrastructure, such as the internet, to provide **remote** offices or individual users with secure access to their organization's network. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

5. POLICY

DoIT provides secure offsite remote access capabilities for selected employees, contractors and other authorized users to access DoIT's network and computers. All remote access to DoIT's network and computers is required to go through the approved, secure remote access facilities provided by the agency and is limited to use for official business.

Remote access capability is provided where there is a need for offsite connections for businesspurposes, such as working from home, business traveling, and vendor support functions. Whenconnecting remotely, employees must abide by all other DoIT policies.

The following requirements are to be followed when remotely connected:

a. Department Managers and DoIT Network Security Teams must explicitly approve all remote access for employees, contractors, vendors, and consultants.

b. Individuals wanting to have remote access capability must complete appropriate request forms and obtainthe required approvals.

c. Third-party vendors providing technical support to DoIT software systems will only be given remote access privileges if approved by the CISO or CIO designee. These privileges will be disabled when not in use and enabled only for the specified timeframe to accomplish the necessary tasks.

d. Secure remote access technology and applications must be used. Strong authentication processes, such multi-factor authentication (MFA) utilizing hard or soft tokens (i.e. software-based MFA), must be used for remote connections to DoIT network and computers. Remote connections must be encrypted. Technologies such as SSH, VPN, or SSL/TLS for web-based management must be utilized. If strong authentication capability is not available for certain approved devices, such as for mobile devices (tablets, smart phones), then the available security features must be activated and used. Such features include device passwords, remotelockout or remote file/configuration delete capability.

e. Remote access controls are to be set to disconnect a connection after a specified amount oftime. The system must also disconnect the connection after 15 minutes of inactivity.

f. The system must prohibit any copying, moving, and storage of confidential information to thelocal machine or local device during a remote connection.

g. At no time should any DoIT employee provide their login or authentication credentials toanyone or allow another person to use their remote access connection.

h. All computers connected remotely to the internal DoIT network are required to use the mostup-to-date anti-virus software and must be protected by a firewall or equivalent software onthe client computer.

i. Organizations or individuals requesting non-standard remote access solutions to DoIT production networks are required to obtain prior approval from the DoIT Chief InformationSecurity Officer (CISO) or CIO designee.

5.1. Inactive Use

Users who have not used their remote access for over 90 days will have their remote access capabilities revoked. In these situations, any multi-factor tokens are to be returned to employee's manager. Exceptions will be based on user's manager's request and CISO or CIO designee approval.

5.2. Shredding

Anyone who is working remotely and printing paper documents on remote printers, or has confidential documents at remote site, must ensure such confidential documents are properly shredded when discarded. Intermediate work products containing confidential information, such ascarbon copies, photocopies, or paper memo drafts, must also be shredded. Remote users on the road must not throw away DoIT confidential information in hotel wastebaskets or other publicly accessible trash containers. Confidential information must be retained until it can be shredded or destroyed.

5.3. Remote Access Revocation

Access may be revoked at any time for reasons not limited to, but including non-compliance with security policies, request by the user's supervisor, or negative impact on overall network performance attributable to remote connections. DoIT IT resource users must at all times protectDoIT information in a manner commensurate with its sensitivity and criticality.

5.4. Remote Access into Customers Environments

DoIT may provide software to customers and may occasionally need to provide technicalsupport via remote access to the customers' site. All such remote access to customer sites isrequired to use a unique authentication credential for each customer.

DoIT will ensure protections to prevent the ability of a remote client accessing multiple VPN tunnels at once while connected to the State of New Mexico VPN(s), unless an appropriate business case is provided.

NMAC 1.12.20.16 USER AUTHENTICATION FOR EXTERNAL CONNECTIONS (REMOTE ACCESS CONTROL):

A. To maintain information security, agency must require through published policies and procedures consistent with these rules, that individual accountability shall be maintained at all times, including during **remote** access.

B. Connection to the agency's networks shall be provided in a secure manner to preserve the integrity of the network, to preserve the data transmitted over that network, and to maintain the availability of the network. Security mechanisms shall be in place to control **remote** access to agency systems and networks from fixed or mobile locations.

C. Approval for any such **remote** connection shall first be obtained from the agency management and the agency CIO or ISO. Prior to approval being granted, the CIO shall review the request to determine what needs to be accessed and what method of access is desired and document the risks involved and technical controls required for such connection to take place.

D. Because of the level of risk inherent with **remote** access, the agency shall require use of a stronger password or another comparable method of protection prior to allowing connection to any agency network. Users shall be informed that all sessions performed remotely are subject to periodic and random monitoring by the agency.

E. When accessing an agency network remotely, identification and authentication of the user shall be performed by the **remote** access system (VPN) in such a manner as to not disclose the password or other authentication information that could be intercepted and used by a third-party.

F. All **remote** connections to an agency computer shall be made through managed central points-of-entry or “common access point.” Using this type of entry system to access an agency computer provides simplified and cost-effective security, maintenance, and support.

G. Vendors which may be provided access to agency computers or software, will be required to have individual accountability. For any agency system (hardware or software) for which there is a default user ID or password that came with the system for use in set up or periodic maintenance of the system, that account shall be disabled until the user ID is needed and requested. Any activity performed while a vendor user ID is in use shall be logged on the **remote** access system by an external logger. Since such maintenance accounts are not regularly used, the vendor user ID shall be disabled, the password changed, and other controls shall be implemented by the agency to prevent or monitor unauthorized use of these privileged accounts during periods of inactivity.

H. In special cases wherein servers, storage devices, or other computer equipment has the capability to automatically connect to a vendor in order to report problems or suspected problems, the agency ISO shall review any such connection and process to report certain events back to the system's manufacturer for performance “tuning” to ensure that such connectivity does not compromise the agency or other third-party connections.

I. Agency personnel will only be allowed to work from a **remote** location upon authorization by the CIO and agency management. Once approved, appropriate arrangements shall be made pursuant to agency written policy and procedures, consistent with this rule, to ensure the work environment at the **remote** location provides adequate security for transmission of agency data and protection of computing resources. The agency shall identify to the user the appropriate protection mechanisms necessary to protect against theft of agency equipment, unauthorized disclosure of agency information, misuse of agency equipment, unauthorized access to the agency internal network, or facilities by anyone besides the specifically identified and approved user, including family and friends. To ensure the proper security controls are in place and all state security

standards are followed, the agency will approve **remote** access after consideration and documentation of their review following:

1) the physical security of the **remote** location, including the use of any portable devices at any location other than an employee's approved work station;
2) the method of transmitting information given the sensitivity of agency's internal system; and
3) clearly defined business continuity procedures, including the capability of backing up critical information.

J. The following access system controls shall be implemented. Agency ISO or CIO shall monitor and audit their use:

1) a definition of the type of information accessed (such as sensitive or confidential information under HIPAA) and the systems and services that the **remote** user is authorized to access;
2) procedures and end user system requirements for secure **remote** access, such as authentication tokens or passwords, shall be documented by the agency including provisions for revocation of authorization and return of equipment to the agency;
3) access system support and usage procedures provided to the users;
4) implementation of suitable network boundary controls to prevent unauthorized information exchange between agency networks connected to **remote** computers and externally connected networks, such as the internet; such measures shall include firewalls and intrusion detection techniques at the **remote** location; and
5) physical security of the equipment used for **remote** access (e.g. securing any remote access device by locking, such as cable locking device, or locking device in cabinet/secure storage area).

6. ROLES AND RESPONSIBILITIES

a. DoIT Network Security Team

The DoIT Network Security team is responsible for usage monitoring and user audits. DoITUsers and Contractors are responsible for adhering to this policy.

7. EXCEPTIONS

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

8. VIOLATIONS OF POLICY

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any vendor found to have violated this policy may be subjectto further action.

9. REFERENCES

a. Payment Card Industry Data Security v3.2: 8.1.5, 8.3, 8.5.1, 12.3.8, 12.3.9, 12.3.10

b. National Institute of Standards and Technology SP800-53 r4: AC-2(3), AC-12, AC-17, IA-2(11), IA-5(11), MA-2(3), SC-7(7)

c. International Organization for Standardization/International Electrotechnical27002:2013: 6.2.2

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
06/10/2021	4	Olga Serafimova, Esq.	Reviewed and revised for legal compliance
05/06/2022	5	Brenda Fresquez	Reviewed for quality assurance

Approval

DocuSigned by:
437214FBE82C453...

6/15/2022

Raja Sambandam, Acting Cabinet Secretary **Date**