



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

Policy Title:	Network Device Configuration Policy
Policy Number:	DoIT-361-711
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.

2. PURPOSE

This Policy establishes base configuration standards for internal network devices such as routers and switches that connect to a DoIT network.

3. SCOPE

This Policy covers all configuration standards for DoIT owned network routers and switches.

4. DEFINITIONS

- a. **Access Control List (ACL)** – A table of acceptable users, groups, or IP addresses that are provided access to a DoIT information system or network.
- b. **DoIT IT Resource Users** - All DoIT employees, contractors, and any other users of DoIT IT resources.
- c. **Router** - A device that forwards data packets along networks based on configured routes and ACL. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect.
- d. **Switch** – A device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model and therefore support any packet protocol. LANs that use switches to join segments are called *switched LANs* or, in the case of Ethernet networks, *switched Ethernet LANs*.
- e. **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.
- f. **Test Network** – A network used for the purposes of testing, demonstration, and training to prevent a disruption in the Production Network.

5. POLICY

DoIT develops, documents, and standardizes configurations for routers and switches. These standards include security configurations that block unwanted access to the network and remove unnecessary

Network Device Configuration Policy – DoIT-361-711

services, ports, and protocols.

Router configuration standards include:

- a. All local account passwords are changed per DoIT's password standard.
- b. Passwords meet DoIT complexity requirements and are updated on a regular basis.
- c. User session will automatically lock after a DoIT defined length of inactivity, if applicable.
- d. Network administrative accounts will automatically log off or terminate from network devices after a DoIT defined length of inactivity.
- e. Users will be locked out after at most 3 invalid login attempts.
- f. Third party vendors do not have access to usernames and passwords unless an Acceptable Use Policy, a vendor contract, and/or a non-disclosure agreement has been signed.
- g. The enabled password on the router must be kept in a secure encrypted form.
- h. Routers' enabled passwords are set to the current production router password from the router's support organization.
- i. A "System Use" banner or notification will be shown when an administrator logs into the network device, notifying them of their responsibility for managing the device as well as possible repercussions for violating the Policy.
- j. Routers must be configured to restrict any connections between untrusted networks and trusted networks, as well as segmented areas with confidential information.
- k. Unnecessary and insecure ports, services, and protocols must not be used.
- l. Documented business justifications are required for any use of services, ports, and protocols.
- m. The following must be disallowed:
 - i. Internet Protocol directed broadcasts;
 - ii. Incoming packets at the Router sourced with invalid addresses, such as RFC1918 address;
 - iii. Transmission Control Protocol small services;
 - iv. User Datagram Protocol small services;
 - v. All source routing;
 - vi. All web services running on Routers; and
 - vii. Use of Agency standardized Simple Network Messaging Protocol community strings.
- n. All Routers are required to have full control over traffic limitation using ACLs.
 - i. ACLs should be used in secure areas where limited access is allowed and to restrict traffic to only allow permitted services and hosts wherever possible.
- o. All Router and Switch rules/configuration settings must be reviewed at a minimum every six months.
- p. Router 'start-up' files are required to be updated and synched with current configuration standards (for example, running files are synched with start-up files).
- q. Physical access to all DoIT Routers must be secured and limited to authorized administrators.

Switch standards include:

- a. All local account passwords are changed per DoIT password standard.
- b. Passwords meet DoIT complexity requirements and are updated on a regular basis.
- c. User session will automatically lock after a DoIT defined length of inactivity, if applicable.
- d. Network administrative accounts will automatically log off or terminate from network devices after a DoIT defined length of inactivity.
- e. Users will be locked out after, at maximum, three (3) invalid login attempts.

Network Device Configuration Policy – DoIT-361-711

- f. Third party vendors do not have access to usernames and passwords unless an Acceptable Use Policy, a vendor contract and/or a non-disclosure agreement has been signed.
- g. The enabled password on the Switch must be kept in a secure encrypted form.
- h. VLAN configurations must be configured according to best practices.
- i. Physical access to all DoIT Switches must be secured and limited to only authorized administrators.
- j. A “System Use” banner or notification must be shown when an administrator logs into the network device, notifying them of their responsibility for managing the device as well as possible repercussions for violating the Policy.
- k. Switches must be managed via DoIT’s standard network management system and have a designated point of contact.

6. ROLES AND RESPONSIBILITIES

- a. **DoIT CISO**
The DoIT Chief Information Security Officer (CISO), the State Chief Information Officer (CIO), or a CISO or State CIO designee is responsible for ensuring all network device policies and standards are adhered to.
- b. **DoIT Network Team Manager**
The DoIT Network Team Manager is responsible for ensuring Network Administrators follow this Policy and for enforcement of this Policy.
- c. **DoIT Network Administrators**
DoIT Network Administrators are responsible for adhering to the requirements established in this Policy.

7. EXCEPTIONS

The DoIT CISO or CIO 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. Payment Card Industry Data Security Standard v3.2: 1.1,2,3,5
- b. National Institute of Standards and Technology SP800-53 r4: AC-2(5), AC-4, AC-7, AC-8, AC-11, AC-12, CM-3, CM-6, SC-7
- c. International Organization for Standardization/International Electrotechnical 27002:2013:13.1.3.

Network Device Configuration Policy – DoIT-361-711

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, Esq.	Reviewed and revised for legal compliance
09/21/2021	5	Olga Serafimova, Esq.	Performed final review and editing
4/27/2022	6	Brenda Fresquez	Reviewed for quality assurance
12/18/2023	6.1	Brenda Fresquez	Annual Review; updated header and footer
12/18/2023	6.1	Bryan E. Brock	Annual Review for legal compliance; no recommended changes

Approval

DocuSigned by:

 437214FBE82C453...

Raja Sambandam, Acting Cabinet Secretary

12/20/2023

Date