NM DEPARTMENT OF
INFORMATION
TECHNOLOGY

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

Policy Title:	**Systems Configuration Policy**
Policy Number:	**DoIT-361-716**
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 baseline configuration standards for DoIT IT equipment including servers, workstations, laptops, networks, and other computer-related devices. All IT devices must be configured, implemented, and maintained in a standardized and secure fashion to reduce risks andenhance security of the IT systems.

3. SCOPE

This Policy covers all responsibilities and configuration standards for DoIT IT devices including the hardware and software of servers, workstations, laptops, networks, and other computer-related devices. Firewall and router configurations are covered in their respective configuration policies.

4. DEFINITIONS

a. **Access Control List (ACL)** – A table of acceptable users, groups, or IP addresses that areprovided access to the information system or network.

b. **DoIT IT Resource Users** – All DoIT employees, contractors, and users of DoIT IT resources.

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

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

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

f. **NT File System (NTFS)** – A proprietary journaling file system developed my Microsoft, whichis the default file management system of the Windows NT family.

g. **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.

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

i. **Server** – A physical/virtual device or program that can host DoIT's and client's services or applications.

j. **Simple Network Management Protocols** – A protocol for collecting and organizing information about a managed device on IP networks (*e.g.*, servers, network devices, etc.).

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

l. **Test Network** – A network used for the purposes of testing, demonstration, and training, as to prevent a disruption in the production environment.

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

n. **Virtual Private Network (VPN)** – An encrypted network that extends a private networkacross a public network to allow a user to send and receive data as if their computing device were connected to a private network.

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

5. POLICY

DoIT maintains approved configuration standards based on business needs for all IT devices to provide consistent, reliable, and secure configuration of systems. All configurations must be tested, and documentation updated annually and when a change is made. System configurations are up to date and have backup copies to re-configure a device back to the approved standard. Anysystem changes must be approved and tracked in compliance with DoIT's *Change Management Process Policy*.

All devices must be registered within DoIT's inventory management systems. Information in DoIT's inventory management systems must be current. At a minimum, the following information isrequired to positively identify the point of contact:

a. Device contact(s) and location, and a backup contact

b. MAC address, IP address, and asset inventory tag

c. Hardware and Operating System/Version

d. Main functions and applications, if applicable; and

e. Asset assignment and ownership.

5.1. General Configuration Requirements

a. All system configurations will incorporate security engineering and hardening principles in the development lifecycle of each system managed by DoIT.

b. Operating System configurations should be in accordance with DoIT's *Information Security Policy* and based on best practice standards, such as one or more of the following:

i. Security Technical Implementation Guides (STIGs)
ii. Center for Internet Security (CIS)
iii. International Organization for Standardization (ISO)
iv. Sysadmin Audit Network Security (SANS)
v. National Institute of Standards Technology (NIST)
vi. IRS Office of Safeguards Safeguard Computer Security Evaluation Matrix (SCSEMs).

c. User sessions will automatically lock the desktop after a DoIT defined length of inactivity andcan only be unlocked by re-entering the valid password.

d. Users will be locked out after 3 invalid login attempts.

e. Unnecessary services and applications must be disabled.

f. Access to services must be logged and protected through access-control methods suchas TCP Wrappers or ACLs, where possible.

g. Vendor patches will be applied as deemed necessary in accordance with DoIT's *Patching and Updating Policy* and risk-rating.

h. Trust relationships between systems are a security risk and their use should be avoided. Trust relationships must not be used when some other method of communication is sufficient.

i. Standard security principles of least required access to perform a function must be used.

j. Root/administrator accounts must not be used when a non-privileged account is sufficient.

k. If a methodology for secure channel connection is available that is technically feasible,privileged access must be performed over secure channels; for example, encrypted networkconnections using SSH or IPsec.

l. Servers, network, infrastructure, and other critical IT devices should be physically located in an access-controlled environment.

m. Servers, network, and infrastructure devices are specifically prohibited from operating from uncontrolled cubicle areas unless approved by the DoIT Chief Information Security Officer (CISO).

n. A current configuration copy (backup) of all devices that connect to the network must be maintained.

5.2. Compliance

a. Audits and security assessments will be performed on a regular basis by authorizedpersonnel within DoIT or approved third parties.

b. Audits and assessments shall verify configuration standards are defined and consistently used, IT devices are securely configured, and configurations are reviewed and maintained periodically.

5.3. Workstation and Laptop Configurations

Every workstation acquired by DoIT must be configured (hardened) to promote a secure posture of the device prior to deploying it to the functional environment. DoIT must decide on thebaseline applications and which applications are necessary for each job description. DoIT shall create images or scripts to modify all configurations to a secure standard. Any changes to images orscripts shall be documented and tested prior to deployment. The following must be addressed for allworkstation and laptop configurations:

a. A “System Use” banner or notification shall be shown when a user logs onto the workstation or laptop, notifying them of their responsibility for managing and use of the device, as well as possible repercussions for violating any policy.

b. The systems need to be configured on the concept of least privilege. Security measures mustbe enforced through the configurations, such as enforcing password length and complexity requirements, closing unused network ports, and patching procedures.

c. DoIT will maintain a list of authorized software and utilize a policy to prevent the installation of unapproved software, which will be reviewed and updated annually.

d. Additional system configurations should address:

i. Components the end-users can utilize (*e.g.*, add/remove programs options)

ii. Features that should be enabled (*e.g.*, Windows Update)

iii. Services that need to be enabled

iv. ACLs; and

v. Firewall Configurations.

5.4. Server Configurations

Server configuring (hardening) must be conducted prior to deployment. DoIT shall document all information regarding the server. For example, MAC address, IP address, machine name, asset tag, and administrator name. DoIT must assure that the following prerequisites are met prior to Hardeningthe system:

a. Operating system and post-operating system software are from legitimate, trusted sources

b. The Server will be connected to a completely trusted network throughout the Hardening process

c. All current service packs and updates are installed.

The hardening process must include adjusting the auditing and account policies and security settings to meet the specified needs of DoIT. The server must be configured to meet the regulatory standards required by government mandates. Configurations should be conducted in the following order:

a. Auditing and Account Policies (Password Settings and Event Logs)

b. Security Settings (account configurations, encryption, log-on banners, anonymousconnections)

c. Security Protections (disable unused services/user accounts, ensure NTFS file systems,firewall configurations, file and registry permissions)

d. Additional Steps (anti-virus/spyware installation and updates, inactivity configurations,disable boot order changes to alternate media).

After configuring the server to meet DoIT needs, any changes or modifications to the server must be approved, documented, and tested to verify the security posture is retained. DoIT shall conduct internal and external assessments to verify security and compliance requirements are met. DoIT must conduct assessments using automated tools to identify any vulnerabilitythat may still exist within the system.

If possible, segregation of information on each server shall be done based on the criticality of information. Each server shall support a given function and be secured appropriately in accordance with criticality of the system or information stored on the server. Any server that holds confidentialinformation shall be encrypted and access to the server shall be via various technologies such as SSH, VPN, or SSL/TLS.

5.5. Various Computing Device Configurations

Any devices connected to the DoIT network (*i.e.*, any device with an IP address assigned) needs to be configured properly to mitigate any risks of being compromised. Devices include, but are not limited to, the following:

a. Routers/Switches
b. Network Printers
c. Scanners
d. Fax Machines
e. VOIP (Telephones)
f. IP Security Cameras

In some situations, these devices may run various services, making turning off all unnecessary services essential. Configuring the device to perform business desired capabilities should address the following:

a. Disable all unnecessary protocols;
b. Assign static IP addresses to devices;
c. Allow access to device via particular subnets;
d. Remove all default passwords and SNMP community strings;
e. Upgrade all patches and firmware;
f. Ensure that logs are being generated on devices;
g. Maintain a physically secure area around the device.

The firewall and router must be configured to restrict or control any connections between un-trusted networks and any information systems containing confidential information. Refer to DoIT's *FirewallPolicy* and *Network Device Configuration Policy*.

All configurations must remain confidential to DoIT. Incorporating these configuration standards oneach device on the network will increase DoIT's security posture.

5.6. Asset Decommissioning

The decommissioning of assets should ensure:

a. The assets to be decommissioned and/or destroyed follow the change control process consistent withDoIT's *IT Change Management Policy* for appropriate record keeping and approval; and

b. All records are immediately updated to reflect the decommissioned assets and notifyrelevant stakeholders.

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 informationsystem device policies and standards are adhered to.

b. DoIT Infrastructure Administrators

DoIT Infrastructure Administrators are responsible for adhering to the requirementsestablished in this Policy.

c. DoIT Infrastructure Team Manager

The DoIT Infrastructure Team Manager is responsible for ensuring that Infrastructure Administrators follow this Policy and enforcement of this Policy.

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 Special Publication SP800-53 r4: AC-7, AC-8, AC-11, AC-11(1), CM-2, CM-3, CM-4, CM-6, CM-7(4), MA-2, MP-6(1), SA-8

b. COBIT v5.0

c. IASE DISA Security Technical Implementation Guides (STIGs)

d. Center for Internet Security (CIS) Benchmarks

e. Sysadmin Audit Network Security (SANS) Critical Security Controls

f. IRS Safeguards Computer Security Evaluation Matrix (SCSEM); and

g. National Institute of Standards and Technology Special Publication 800-128, Guide forSecurity-Focused Configuration Management of Information Systems.

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
06/10/2021	4	Olga Serafimova, Esq.	Reviewed and revised for legal compliance
09/20/2021	5	Olga Serafimova, Esq.	Performed final review and editing
05/26/2022	6	Brenda Fresquez	Reviewed for quality assurance

Approval

DocuSigned by:

437214FBE82C453...

6/15/2022

Raja Sambandam, Acting Cabinet Secretary

Date