NM DEPARTMENT OF INFORMATION TECHNOLOGY

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

Policy Title:	**Information Systems Logging and Monitoring Policy**
Policy Number:	**DoIT-361-708**
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 1.12.20.22(A) NMAC, and consistent with applicable law, DoIT reserves the right to monitor, inspect, and search at any time, all DoIT information systems and equipment used by DoIT IT Resource Users. Since agency computers and networks are provided for state business purposes, DoIT IT Resource Users, including contractors specifically allowed limited use of state systems or equipment, shall have no expectation of privacy with regard to the information stored in or sent through the state information systems. DoIT may remove from its information systems any material unauthorized by DoIT or by state statute.

2. PURPOSE

This Policy establishes requirements for logging and monitoring systems, security, and network activities to ensure appropriate use of computer resources and to provide a means to trace activities back to specific users.

3. SCOPE

This Policy applies to all DoIT information technology (IT) Resource Users and all network, applications, and security resources.

4. DEFINITIONS

a. **DoIT IT Resource Users** - All DoIT employees, contractors, and any other users of DoIT IT resources.
b. **Intrusion Detection System** – Device or software application that monitors an information system for malicious activity or policy violations.
c. **Intrusion Prevention System** – Network security system that detects and prevents identified cyber threats.

NMAC 1.12.20.32 LOG-ON BANNER:

A. Log-on banners shall be implemented on all state IT systems to inform all users that agency systems are only for agency business and other approved uses consistent with agency policy, to inform that users their activities may be monitored, and to inform the user that they have no expectation of privacy.

B. Logon banners shall be displayed on computer screens during the authentication process. [1.12.20.32 NMAC - N/E, 04/14/2010]

NMAC 1.12.20.33 MONITORING SYSTEM ACCESS AND USE: NO EXPECTATION OF PRIVACY:

A. Systems and applications shall be monitored and analyzed by agency ISO or agency designated IT staff to detect deviation from the state access control policy.

B. Events shall be recorded to provide evidence of misuse and to reconstruct lost or damaged data by the agency system administrator.

C. Audit logs shall be used to record user activities and other security-relevant events.

D. Audit log reports shall be produced to agency CIO and ISO and kept consistent with agency record retention schedules.

5. POLICY

DoIT logs system data and activity on network infrastructure to provide a history of network interactions and behavior. DoIT Network Security Team analyze network, systems, and applicationscomponents to identify audit logging functions and capabilities, and to identify required logs to enable and monitor critical systems.

5.1. Audit Logs

The following are the minimum standards for implementing and monitoring audit logs:

a. Enable audit logs that link individual user access to confidential information, customerinformation, or critical systems.

b. For network and application systems, log all:

i. Access to confidential, sensitive, and customer information;
ii. Actions taken by user accounts with administrative or root privileges;
iii. Access to audit logs;
iv. Invalid access attempts;
v. User account adds, changes and deletions/ disabling and other security administrative changes;
vi. Changes to user accounts with administrative or root privileges;

vii. Initialization, stopping or pausing of audit logs;
viii. Creation and deletion of system-level objects;
ix. Changes to security configuration parameters and system configuration settings; and
x. Security events (e.g., anti-virus, Intrusion Detection System/Intrusion PreventionSystem, firewall, etc.).

c. For each log event, record at least the following data elements:
i. User account identification;
ii. Type of event;
iii. Date and time which will be timestamped in either GMT or UTC;
iv. Success or failure of event;
v. Origination of event; and
vi. Identity or name of affected data, system component or resource.

5.2. Security of logs

To institute separation of duties, audit logs are protected from alteration and unauthorized access.

a. Access, including read only, to the audit logs is restricted to authorized personnel only.
b. Logs are protected from unauthorized modifications via access control mechanisms,segregation or other similar techniques.
c. Logs are promptly backed up to a centralized log server or other media that is hard toalter.
d. Logs for externally facing systems are written to a secure, centralized internal log server ormedia device.
e. File integrity monitoring software is used on logs to ensure log data is not changed.
f. System administrator permission to erase or de-activate logs of their own activities isrestricted.

5.3. Monitoring and Review

Monitoring is the act of reviewing system logs, inspecting log events, and continuously monitoringthe information systems to ensure that information resources are used in compliance with their intended use and to detect anomalies or suspicious activities.

Audit logs are routinely reviewed. The following are reviewed daily:

a. All security events.
b. Logs of system components that store confidential data.
c. Logs of critical systems.
d. Logs of servers and systems that perform security functions.

Reviews may be automated so that the suspicious activities are identified and alerted to personnel. Other system logs are to be reviewed periodically, based on risks and business needs.

Information systems will continuously monitor the following metrics and utilizations at minimum:

a. Uptime
b. Processor
c. Memory
d. Storage
e. Network

DoIT Network Security Team will receive the notifications if monitoring thresholds have been triggered.

5.4. Time Sync

The clocks of all relevant information processing systems must be synchronized with an agreed accurate time source that are stored as Greenwich Mean Time (GMT) or Coordinated Universal Time(UTC) time.

5.5. Retention

Audit logs must be retained for at least 90 days or longer based on regulatory requirements.

6. ROLES AND RESPONSIBILITIES

a. DoIT CISO

The DoIT Chief Information Security Officer (CISO) or Chief Information Officer (CIO) designee is responsible for ensuring the retentionof logs as they adhere to compliance mandates.

b. DoIT Network Security Team

The DoIT Network Security Team is responsible for the review of event logs and determininga course of action when deemed appropriate.

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. Payment Card Industry Data Security Standards v3.2: 10.1,2
b. National Institute of Standards and Technology SP800-53 r4: AU-2, AU-2(3), AU-3, AU- AU-4, **AU-5, AU-6, AU-6(1), AU-6(5), AU-8, AU-9, AU-11, AU-12, CA-7**
c. International Organization for Standardization/International Electrotechnical Commission 27002:2013: 12.4

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
06/29/2021	4	Olga Serafimova	Reviewed and revised for legal compliance
12/28/2021	5	Brenda Fresquez	Proofread for quality assurance

Approval

DocuSigned by:
437214FBE82C453...

6/27/2022

Raja Sambandam, Acting Cabinet Secretary **Date**