



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

Policy Title:	Incident Response Policy
Policy Number:	DoIT-361-707
Effective Date:	3/21/2022
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 1.12.20.8 NMAC, all agency information technology (IT) technical operations shall have documented security operating instructions, management processes, and formal incident management procedures in place that define roles and responsibilities of individuals who operate or use agency IT technical operations and facilities.

Per 1.12.24(F) NMAC, all documents pertaining to security investigations shall be categorized as sensitive and protected from public disclosure.

2. PURPOSE

This Policy establishes an Incident Response Team (IRT) and associated processes required to respond to any computer security incident to minimize any loss due to destruction, mitigate any weakness exploited, restore computing services as required, and track and report on security incidents or customer data breaches.

3. SCOPE

This Policy applies to all DoIT IT Resource Users and covers computer security incidents and privacy incidents across DoIT computer systems and networks and supports compliance requirements for reporting incidents to appropriate authorities and affected customers.

4. DEFINITIONS

- a. **DoIT IT Resource Users** - All DoIT employees, contractors, and other users of DoIT IT resources.
- b. **Computer Security Incident** - Any network or host activity that potentially threatens the security of computer systems; any real or suspected adverse event in relation to the security of computer systems or computer networks.
- c. **Data Breach Incident** – Any event resulting in compromise of DoIT or DoIT customer data, including but not limited to: unauthorized release, loss, or theft of data; unauthorized access to or use of data; and/or misplacement, public display or accidental disclosure wherein such event results in substantial harm or

Incident Response Policy - DoIT 361-707

inconvenience to DoIT or the customer(s).

- d. **Personally Identifiable Information (PII)** - Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.
- e. **Privacy Incident** - Only those incidents that relate to Personally Identifiable Information (PII).

5. POLICY

DoIT is required to create and maintain an Incident Response Plan, and to establish an IRT whose members participate in reviewing, approving, and executing the Plan. The DoIT Chief Information Security Officer (CISO) appoints IRT members and oversees their work in accordance with the Plan. The IRT may bring in additional resources as needed to investigate computer-related incidents and/or DoIT or customer data information incidents. At a minimum, the IRT will include:

- a. DoIT CISO – Response Plan Owner, Response Team Lead;
- b. Enterprise Services Management;
- c. SHARE Management;
- d. Human Resources;
- e. Legal; and
- f. Forensics team (can be third party).

The DoIT Incident Response Plan addresses computer security incidents and customer data breaches and must cover, at a minimum:

- a. Roles and responsibilities;
- b. Communications strategies and processes regarding:
 - i. DoIT personnel;
 - ii. Regulatory agencies;
 - iii. Law enforcement;
 - iv. Public and news media; and
 - v. Individual(s) whose data has definitely or potentially been compromised;
- c. Procedures for detection, analysis, containment, eradication and recovery;
- d. Data backup processes;
- e. Incident response procedures, training, and testing and exercises covering lessons learned from previous incidents and from on-going incident handling activities; and
- f. Analysis of legal requirements for reporting compromises.

DoIT's incident response capability must be tested at least annually using checklists, walk-throughs, tabletop exercises, simulations, and/or comprehensive exercises to determine IRT and process effectiveness. The DoIT CISO documents the results of the annual testing and is responsible for ensuring completion of follow-up efforts to improve the agency's incident response preparedness.

DoIT will provide incident response training relevant to assigned duties annually and will provide privacy incident training to staff responsible for PII.

6. ROLES AND RESPONSIBILITIES

a. DoIT CISO

The DoIT CISO or a CIO designee is responsible for:

Incident Response Policy - DoIT 361-707

- i. Establishing the IRT and ensuring members are trained and aware of their responsibilities;
- ii. Creating and maintaining an accurate, up-to-date Incident Response Plan;
- iii. Ensuring the IRT and the Incident Response Plan are subject to at least annual testing and include any related plans as part of the testing process;
- iv. Maintaining documentation and tracking logs that demonstrate how the policy and Plan objectives have been satisfied;
- v. Ensuring that IRT members keep accurate records of actions taken; and
- vi. Leading the IRT in case of an incident or breach.

b. DoIT CIO

The DoIT Chief Information Officer (CIO), or delegated representative, is responsible for initiating the Incident Response Plan. Jointly, the DoIT CISO and the IRT support all related internal, external, and regulatory compliance audits.

c. DoIT IRT

The IRT is responsible for:

- i. Responding to incidents in accordance with the Incident Response Plan;
- ii. Reporting to the CISO on the status of the Plan, on any incidents reported and investigated, and if there are lessons learned to modify the Plan;
- iii. Remediating incidents by performing immediate Risk Assessment and impact analyses to identify proximate and root causes; ensuring appropriate steps are taken to control the situation; and performing Risk Assessments as appropriate to the specific breach (e.g., payment card data, PII); and
- iv. Individually maintaining detailed, accurate records of all actions taken, including but not limited to identification of who took an action, what the action was, and the exact date and time the action was taken.

7. CONFIDENTIALITY

All documents pertaining to security investigations and reports shall be categorized as sensitive and protected from public disclosure, including but not limited to requests for information pursuant to the Inspection of Public Records Act. DoIT's General Counsel shall review and approve such information to ensure compliance with state law.

8. EXCEPTIONS

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

9. 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.

10. REFERENCES

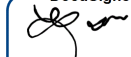
- a. Payment Card Industry Data Security Standards v3.2: 12.10.1-6
- b. National Institute of Standards and Technology 800-61 Rev.2, Computer Security Incident Handling Guide
- c. National Institute of Standards and Technology Special Publication SP800-53 r4: IR-1, IR-2, IR-2(1), IR-3, IR-4, IR-4(1), IR-4(4), IR-5, IR-5(1), IR-6, IR-6(1), IR-7, IR-7(1), IR-8

Incident Response Policy - DoIT 361-707**11. 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
06/03/2021	4	Olga Serafimova	Reviewed and revised for legal compliance
12/28/2021	5	Brenda Fresquez	Reviewed for quality assurance
3/15/22	6	Marko Satarain	No changes, reviewed and accepted by HR—Marko Satarain, Legal—Todd Baran and CWA—Dan Secrist
11/13/2023	6.1	Brenda Fresquez	Annual Review; updated header and footer
11/13/2023	6.1	Bryan E. Brock	Annual Review - Legal. No changes recommended.

Approval

DocuSigned by:



437214FBE82C453...

Raja Sambandam, Acting Cabinet Secretary11/14/2023**Date**