



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

Policy Title:	Acceptable Use of IT Resources
Policy Number:	DoIT-361-701
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.

Pursuant to NMAC 1.12.10.11, the Secretary of DoIT has discretion to adopt additional DoIT-specific information technology (IT) resource usage Policies that are more restrictive than NMAC 1.12.10.

2. PURPOSE

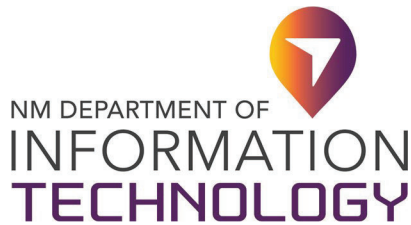
This Policy informs DoIT employees, contractors, and other users of DoIT IT resources of proper use and protection of these resources and data, including but not limited to the internet, the intranet, email, and the State's digital network and supporting systems. This Policy and related procedures protect DoIT systems, maintain compliance with applicable regulations, protect customer information, and reduce business risk.

3. SCOPE

The Policy governs the use of State of New Mexico IT and data telecommunications resources.

4. DEFINITIONS

- a. **access** means the ability to read, change, or enter data using a computer or an information system.
- b. **equipment** means computers, monitors, keyboards, mice, routers, switches, hubs, networks, or any other IT assets.
- c. **freeware or shareware** means software that is available free of charge and available for download from the internet. Freeware is protected by a copyright and is subject to applicable copyright laws.
- d. **information technology resources (IT resources)** means computer hardware, software, databases, electronic message systems, communication equipment, computer networks, telecommunications circuits, and any information used by a State agency to support programs or operations that is generated by, transmitted within, or stored on any electronic media.
- e. **malicious code** means any type of code intended to damage, destroy, or delete a computer system, network, file, or data.



Michelle Lujan Grisham

New Mexico Governor

Raja Sambandam

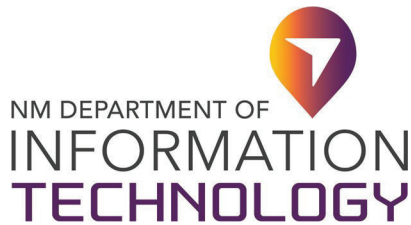
Acting Cabinet Secretary & State CIO

- f. **pirated software** means licensable software installed on a computer system for which a license has not been purchased or legally obtained.
- g. **security mechanism** means a firewall, proxy, internet address-screening or filtering program, or other system installed to prevent the disruption or denial of services or unauthorized use, damage, destruction, or modification of data and software.
- h. **sexually explicit or extremist materials** means images, documents, or sounds that can reasonably be construed as:
 - i. discriminatory or harassing; or
 - ii. defamatory or libelous; or
 - iii. obscene or pornographic; or
 - iv. threatening to an individual's physical or mental well-being; or
 - v. read or heard for any purpose that is illegal.
- i. **user** means any person authorized by DoIT to access State IT resources, including a State employee, officer or contractor; a user for purposes of this rule does not include a person who accesses State telecommunications resources offered by the State for use by the general public.

5. POLICY

The internet and other information technology resources are important assets the State can use to gather information to improve external and internal communications and increase efficiency in business relationships. To encourage the effective and appropriate use of the State's IT resources, the following Policies govern use of the State's IT resources:

- a. DoIT shall provide all users with a written copy of this rule.
 - i. All users shall sign and date a statement indicating they have received and read this Policy.
 - ii. Each user's signed statement shall be kept on file for as long as the user is employed by, has a contract with or otherwise provides services to DoIT.
- b. For purposes of this Policy, IT resources usage includes but is not limited to all current and future internet/intranet communications services, the world wide web, State intranets, voice over IP, file transfer protocol (FTP), TELNET, email, peer-to-peer exchanges, and various proprietary data transfer protocols and other services.
- c. The State of New Mexico may undertake all prudent and reasonable measures to secure the systems it uses for internet communications and the data transmitted by these systems and services, at the direction of the governor or her/his designee(s).
- d. The State of New Mexico and/or its agencies may install software and/or hardware to monitor and record all IT resources usage, including email and web site visits. The State retains the right to record or inspect all files stored on State systems.
- e. State IT resources shall be used solely for State business purposes (except as described in Section 7, below) and users shall conduct themselves in a manner consistent with appropriate behavior standards as established in existing Policies. All State of New Mexico Policies relating to intellectual property protection, privacy, misuse of State equipment, sexual harassment, sexually hostile work environment, data security, and confidentiality shall apply to the use of IT resources.



Michelle Lujan Grisham
New Mexico Governor

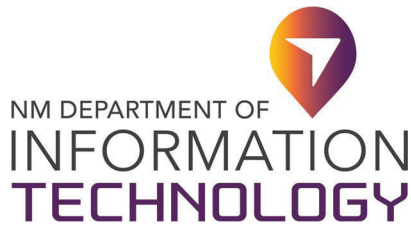
Raja Sambandam
Acting Cabinet Secretary & State CIO

- f. Users shall have no expectations of privacy with respect to State IT resource usage. Serious disciplinary action up to and including termination of employment or contract may result from evidence of prohibited activity obtained through monitoring or inspection of electronic messages, files, or electronic storage devices. Illegal activity involving State IT resource usage may be referred to appropriate authorities for prosecution.

6. PROHIBITED INTERNET USE

State IT resources shall not be used for anything other than official state business unless otherwise specifically allowed by the Secretary of DoIT or as permitted under Section 7, below.

- a. No software licensed to the State nor data owned or licensed by the State shall be uploaded or otherwise transferred out of the State's control without explicit authorization from the Secretary of DoIT.
- b. Resources shall not be used to reveal confidential or sensitive information, client data, or any other information covered by existing State or federal privacy or confidentiality laws, regulations, rules, policies, procedures, or contract terms. Users who engage in the unauthorized release of confidential information via the State's IT resources, including but not limited to newsgroups or chat rooms, will be subject to sanctions in existing Policies and Procedures associated with unauthorized release of such information.
- c. Users shall respect the copyrights, software, licensing rules, property rights, privacy, and prerogatives of others, as in any other business dealings.
- d. Users shall not download executable software, including freeware and shareware, unless it is required to complete their job responsibilities.
- e. Users shall not use State IT resources to download or distribute pirated software or data, including music or video files.
- f. Users shall not use State IT resources to deliberately propagate any malicious code.
- g. Users shall not use State IT resources to intentionally disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of the State's IT resources.
- h. Unauthorized dial-up access to the internet is prohibited from any device that is attached to any part of the State's network. The State's IT resources shall not be used to establish connections to non-State internet service providers without prior authorization in writing by the office of the chief information officer or the State chief information security officer.
- i. Users shall not access, store, display, distribute, edit, or record sexually explicit or extremist material using State IT resources.
 - i. In agencies or offices where the display or use of sexually explicit or extremist materials falls within legitimate job responsibilities, an agency head may exempt a user in writing from the requirements of this subsection. The agency issuing the exemption letter shall keep the letter on file for as long as the user is employed by, has a contract with, or otherwise provides services to the agency.
 - ii. The incidental and unsolicited receipt of sexually explicit or extremist material, such as might be received through email, shall not constitute a violation of this section, provided



Michelle Lujan Grisham

New Mexico Governor

Raja Sambandam

Acting Cabinet Secretary & State CIO

that the material is promptly deleted and neither stored nor forwarded to other parties.

- j. Users are prohibited from accessing or attempting to access IT resources for which they do not have explicit authorization by means of user accounts, valid passwords, file permissions or other legitimate access and authentication methods.
- k. Users shall not use State IT resources to override or circumvent any security mechanism belonging to the State or any other government agency, organization or company.
- l. Users shall not use State IT resources for illegal activity, gambling, or to intentionally violate the laws or regulations of the United States, any state or local jurisdiction, or any other nation.

7. PERSONAL USE OF THE INTERNET

Occasional and incidental personal use of State's IT resources and internet access is allowed subject to limitations. Personal use of the internet is prohibited if:

- a. it materially interferes with the use of IT resources by the State or any political subdivision thereof;
or
- b. such use burdens the State or any political subdivision thereof with additional costs; or
- c. such use interferes with the user's employment duties or other obligations to the State or any political subdivision thereof; or
- d. such personal use includes any activity that is prohibited under this rule.

For additional limitations on personal use of the internet, see Exhibit A to this Policy.

8. ROLES AND RESPONSIBILITIES

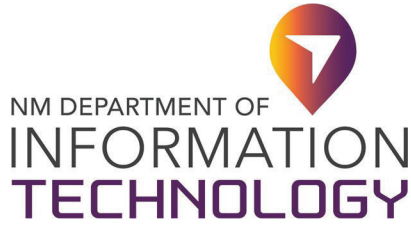
- a. **DoIT CIO and CISO**
The DoIT Chief Information Officer (CIO) and DoIT Chief Information Security Officer (CISO) are responsible for overseeing adherence and enforcement of this Policy.
- b. **DoIT IT Resources Users**
DoIT IT resources Users are responsible for adhering to this Policy, including reporting any potential violation of this Policy to their direct supervisor or to other DoIT senior management staff.

9. EXCEPTIONS

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

10. VIOLATIONS OF POLICY

Any User found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.



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

11. REFERENCES

- a. 1.12.10 NMAC
- b. National Institute of Standards and Technology SP800-53 r4: CM-10, CM-11, MP-7. MP-7(1), PL-4, PL-4(1), SC-19
- c. International Organization for Standardization/International Electrotechnical Commission 27002:2013: 9.3

12. CHANGE HISTORY

Date	Version	Changed By	Change Comments
09/30/2019	1		Initial Draft
02/26/2021	2	Raja S	Revised and routed for Union approval
05/13/2021	3	Olga Serafimova	Reviewed and revised for legal compliance
10/8/2021	4	Brenda Fresquez	Reviewed for quality assurance

Approval

DocuSigned by:

 437214FBE82C453...

Raja Sambandam, Acting Cabinet Secretary

6/27/2022

Date