TITLE 1 GENERAL GOVERNMENT ADMINISTRATION
CHAPTER 12 INFORMATION TECHNOLOGY
PART 10 INTERNET, INTRANET, EMAIL, AND DIGITAL NETWORK USAGE

1.12.10.1 ISSUING AGENCY. Information Technology Commission, 404 Montezuma, Santa Fe, NM 87501.
[1.12.10.1 NMAC - N, 9-15-04]

1.12.10.2 SCOPE. The policy governs the use of state of New Mexico information technology (IT) and data telecommunications resources.
[1.12.10.2 NMAC - N, 9-15-04]

1.12.10.3 STATUTORY AUTHORITY. Section 15-1C-5 NMSA 1978.
[1.12.10.3 NMAC - N, 9-15-04]

1.12.10.4 DURATION. Permanent.
[1.12.10.4 NMAC - N, 9-15-04]

1.12.10.5 EFFECTIVE DATE. September 15, 2004, unless a later date is cited at the end of a section.
[1.12.10.5 NMAC - N, 9-15-04]

1.12.10.6 OBJECTIVE. The purpose of this policy is to provide state of New Mexico staff with guidance on the proper use of the state's information technology resources, including but not limited to the internet, the intranet, email, and the state's digital network and supporting systems.
[1.12.10.6 NMAC - N, 9-15-04]

1.12.10.7 DEFINITIONS. As used in this policy:

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 information technology 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 that is 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;

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 the 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:

(1) discriminatory or harassing; or
(2) defamatory or libelous; or
(3) obscene or pornographic; or
(4) threatening to an individual's physical or mental well-being; or
(5) read or heard for any purpose that is illegal; and

I. **user** means any person authorized by a state agency 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.
[1.12.10.7 NMAC - N, 9-15-04]

1.12.10.8 POLICY. The internet and other information technology resources are important assets that 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 the use of the state's IT resources:

A. State agencies shall provide all users with a written copy of this rule.

(1) All users shall sign and date a statement indicating they have received and read this policy.

(2) 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 the agency.

B. For the purposes of this rule, IT resources usage includes but is not limited to all current and future internet/intranett 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 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 any and all files stored on state systems.

E. State IT resources shall be used solely for state business purposes (except as described in Section 1.12.10.10 NMAC) and users shall conduct themselves in a manner consistent with appropriate behavior standards as established in existing state 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.

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. [1.12.10.8 NMAC - N, 9-15-04]

1.12.10.9 PROHIBITED INTERNET USE. State IT resources shall not be used for anything other than official state business unless otherwise specifically allowed by the agency head or as permitted under Section 1.12.10.10 NMAC.

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 agency head.

B. IT 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 technology security officer.

I. Users shall not access, store, display, distribute, edit, or record sexually explicit or extremist material using state IT resources.

(1) 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.

(2) 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 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.

[1.12.10.9 NMAC - N, 9-15-04]

1.12.10.10 PERSONAL USE OF THE INTERNET. Occasional and incidental personal use of the 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.

[1.12.10.10 NMAC - N, 9-15-04]

1.12.10.11 AGENCY POLICIES. All agencies shall implement this policy immediately upon its effective date. At the discretion of the agency head, an agency may adopt additional agency-specific IT resources usage policies that are more restrictive than this rule, but in no case shall an agency adopt policies that are less restrictive than this rule. This rule shall control in the event of any conflict between an agency policy and this rule.

[1.12.10.11 NMAC - N, 9-15-04]

HISTORY OF 1.12.10 NMAC: [RESERVED]