

EXHIBIT A

EXECUTIVE BRANCH INFORMATION TECHNOLOGY RESOURCES POLICY: INTERNET, INTRANET, EMAIL, AND DIGITAL NETWORK USAGE

- 1 **ISSUING AGENCY.** Office of the Governor, State Capitol, Santa Fe, NM 87503.
- 2 **SCOPE.** The policy applies to all executive branch staff that use State of New Mexico information technology (IT) and data telecommunications resources.
- 3 **STATUTORY AUTHORITY.** NMSA 1978 Sections 10-16-3, 10-16-11, and 15-1C-5.
- 4 **DURATION.** Permanent.
- 5 **EFFECTIVE DATE.** July 17, 2003, unless a later date is cited at the end of a section or paragraph.
- 6 **OBJECTIVE.** The purpose of this policy is to provide executive branch 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.
- 7 **DEFINITIONS.** As used in this policy:
 - 7.1 **access** means the ability to read, change, or enter data using a computer or an information system.
 - 7.2 **equipment** means computers, monitors, keyboards, mice, routers, switches, hubs, networks, or any other information technology assets.
 - 7.3 **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.
 - 7.4 **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.

- 7.5 **malicious code** means any type of code intended to damage, destroy, or delete a computer system, network, file, or data.
- 7.6 **pirated software** means licensable software installed on a computer system for which a license has not been purchased or legally obtained.
- 7.7 **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.
- 7.8 **sexually explicit or extremist materials** means images, documents, or sounds that can reasonably be construed as:
- 7.8.1 Discriminatory or harassing; or
 - 7.8.2 defamatory or libelous; or
 - 7.8.3 obscene or pornographic; or
 - 7.8.4 threatening to an individual's physical or mental well-being; or
 - 7.8.5 read or heard for any purpose that is illegal.
- 7.9 **staff or staff member** means an individual associated with the executive branch who is:
- 7.9.1 An employee holding a classified position authorized by the State Personnel Act; or
 - 7.9.2 an employee exempt from the State Personnel Act; or
 - 7.9.3 an individual working under contract to the state; or
 - 7.9.4 a volunteer providing services to the state, or
 - 7.9.5 a docent providing services at a state museum facility.
- 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 are placed in effect:
- 8.1 Agencies shall provide all staff that have access to information technology resources with a written copy of this policy.
- 8.1.1 All staff shall sign and date a statement indicating they have received and read this policy. This requirement includes all current and future executive agency staff.
 - 8.1.2 Each staff member's agency shall keep the staff member's signed statement on file throughout the tenure of the staff member with that agency.

- 8.2 For the 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.
 - 8.3 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).
 - 8.4 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.
 - 8.5 Staff shall utilize state IT resources solely for state business purposes (except as described in Section 10) and shall conduct themselves in a manner consistent with appropriate behavior standards as established in existing state policies. All existing 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 apply to staff use of IT resources. Staff must also comply with laws governing political speech.
 - 8.6 Staff shall have no expectations of privacy with respect to state IT resource usage. Employees are advised that serious disciplinary action up to and including termination of employment 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.
- 9 PROHIBITED INTERNET USE.** Staff shall not use any state IT resources for anything other than official state business unless otherwise specifically allowed by their supervisor or another authority designated by their Agency Director or Secretary. Personal use of the state's IT resources shall be permitted only in accordance with Section 10 of this policy.
- 9.1 Staff shall not upload or otherwise transfer out of the state's direct control any software licensed to the state nor data owned or licensed by the state without explicit authorization from the manager responsible for the software or data.

- 9.2 Staff shall not use IT resources 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. Staff 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.
- 9.3 Staff shall respect the copyrights, software, licensing rules, property rights, privacy, and prerogatives of others, as in any other business dealings.
- 9.4 Staff shall not download executable software, including freeware and shareware, unless it is required to complete their job responsibilities.
- 9.5 Staff shall not use state equipment to download or distribute pirated software or data, including music or video files.
- 9.6 Staff shall not use state IT resources to deliberately propagate any malicious code.
- 9.7 Staff 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.
- 9.8 Unauthorized dial-up access to the Internet is prohibited from any device that is attached to any part of the state's network. Staff shall not use the state's IT resources to establish connections to non-state internet service providers unless they are authorized to do so in writing by the Office of the Chief Information Officer or the State Chief Information Technology Security Officer.
- 9.9 Staff shall not access, store, display, distribute, edit, or record sexually explicit or extremist material using state IT resources. Violation of this policy may result in immediate disciplinary action as described in Section 11, up to and including termination of employment.
 - 9.9.1 In agencies or offices where the display or use of sexually explicit or extremist materials falls within legitimate job responsibilities, an Agency Director, Secretary, or his/her designee may exempt a staff member in writing from the requirements of Section 9.9. The agency issuing the exemption letter shall keep the letter on file throughout the tenure of the staff member with that agency.

9.9.2 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.

9.10 Staff 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.

9.11 Staff 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.

9.12 Staff 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.

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.

10.1 Personal use of the Internet is prohibited if:

10.1.1 it materially interferes with the use of IT resources by the state or any political subdivision thereof; or

10.1.2 such use burdens the state or any political subdivision thereof with additional costs; or

10.1.3 such use interferes with the staff member's employment duties or other obligations to the state or any political subdivision thereof; or

10.1.4 such personal use includes any activity that is prohibited under this policy.

11 ENFORCEMENT AND SANCTIONS.

11.1 Violations of this policy shall be investigated promptly and efficiently by objective and appropriate staff to be designated by the Agency Secretary or Director.

11.2 Staff suspected of violating this policy shall be given notice of an investigation and an opportunity to present any relevant, exculpatory evidence or mitigating circumstances regarding the charge of the violation.

11.3 If the investigation shows the staff member violated this policy, the staff member may be subject to suspension or termination of access to IT resources, as well as disciplinary action up to and including termination of employment. If the investigation shows the staff member to have engaged in any of the activities prohibited in Sections 9.6, 9.9, or 9.12, disciplinary proceedings will commence in accordance with the State Personnel Act and Rules, and shall include a written reprimand and suspension without pay for at least one week or up to one month, or termination for cause.

12 AGENCY POLICIES. All Executive branch agencies shall implement this policy immediately upon its effective date. At the discretion of the Agency Director or Secretary, an agency may adopt additional agency-specific IT resources usage policies that are more restrictive than this policy, but in no case shall an agency adopt policies that are less restrictive than this policy. Any conflicts found in an Agency policy shall be corrected to be in accordance with this policy.