GENERAL ADMINISTRATION
EMPLOYEE

043 GENERAL OFFICE POLICIES

043.5 Use of State Information Technology Resources Policy

043.5.1 Purpose

The purpose of this policy is to provide staff with guidance on the acceptable use of the Human Services Department's (HSD) information technology resources regarding the protection of the confidentiality, integrity, and availability of those resources.

HSD's information technology resources are and shall remain the property of HSD, subject to its sole control. Improper use of information technology resources poses increased risk to the department and its resources. HSD's staff has the responsibility to safeguard information technology resources.

043.5.2 Definitions

A. "Access" means the ability to read, change, or enter data using a computer or an information system.

B. "Availability" means timely and reliable access and use of information technology resources by an authorized user.

C. "Confidential" or "Confidentiality" means restrictions on information access and disclosure of data including personal privacy and proprietary information.

D. "Confidential Data" This is highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. Explicit authorization by the Data Owner is required for access because of legal, contractual, privacy, or other constraints. Unauthorized disclosure could have a serious adverse impact on the business of HSD or affiliates, the personal privacy of individuals, or on compliance with federal or state laws and regulations or HSD contracts. Confidential data types require a very high level of security controls. Examples include but, are not limited to:

- Income tax records (FTI)
- Medical records (PHI)
- Personally Identifiable Information (PII).
- Social Security Number
- Date of birth
- Financial Information
- Place of birth
- Driver license numbers
- Mother's maiden name

- Credit card numbers
- Bank account numbers
- Personal address
- Authentication tokens (e.g., personal digital certificates, passwords, etc.)

E. "Equipment" means computers, monitors, keyboards, mice, routers, switches, hubs, networks, or any other information technology assets.

F. "Federal Tax Information" (FTI) means federal taxpayer returns and tax return information. The IRS requires that appropriate safeguards are maintained to protect confidentiality of FTI.

G. "Freeware", "Open-Source" 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.

H. "Information Technology Resources" (IT Resources) means computer hardware, software, databases, electronic message systems, communication equipment (including USB memory sticks), computer networks, all current and future internet, intranet and telecommunications circuits, and any information that is used by HSD to support programs or operations that is generated by, transmitted within, or stored on any electronic media.

I. "Integrity" means accuracy and authenticity of the information within IT resources.

J. "Malicious Code" means any type of code intended to damage, destroy, or delete a computer system, network, file, or data.

K. "Materially Interferes" means such use burdens the department or state with additional costs, or interferes with the user's employment duties or other obligations to the department or state.

L. "Personally Identifiable Information" (PII), as used in information security, is information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify, contact, or locate a single individual. Examples are full name, driver's license number, social security number.

M. "Pirated Software" means licensed software installed on a computer system for which a license has not been purchased or legally obtained.

N. "Protected Health Information" (PHI), also referred to as Personal Health Information, means information that identifies a single individual or describes the individual's past, present or future physical or mental health condition.

O. "Removable Media" are data storage devices capable of computer system removal without powering off the system. Removable media devices are used for backup, storage or transportation of data. Examples include but, are not limited to; USB drives, CDs, Memory Cards, Disk packs, external hard drives, Digital cameras, and Smart Phones.

P. "Security Incident" the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Q. "Security mechanism" means IT resources to prevent the disruption or denial of services or the unauthorized use, damage, destruction, or modification of data and software.

R. "Sexually explicit", "extremist materials", and "libelous and defamatory material" means:

1. "Sexually explicit" material is material that the average person would find, applying contemporary community standards, appeals to the prurient interest. It is material that depicts or describes, in a patently offensive way, sexual conduct specifically defined by applicable New Mexico law, and taken as a whole, lacks serious literary, artistic, political or scientific value.

2. "Extremist material" is material which advocates resorting to violence or other unlawful action, particularly with respect to achieving the objectives of political, racial or religious ideologies. It includes material advocating violent or otherwise unlawful action toward groups or individuals based on race, religion, gender, sexual orientation, national origin or political views.

3. "Libelous and defamatory material" is material that contains any false and malicious statement affecting the reputation, business or occupation of another, or which exposes another to hatred, contempt, ridicule, degradation or disgrace and which is circulated without good motives and justifiable ends.

This also means images, documents, or sounds that can reasonably be construed as:

1. Discriminatory or harassing; or

2. Obscene or pornographic; or

3. Threatening to an individual's physical or mental well-being; or

4. Read or heard for any purpose that is illegal

S. "Staff" or "Staff Member" means:

1. An individual working for the Human Services Department

2. An individual working under contract or as a vendor to the state

3. A volunteer providing services to the state

043.5.3 Policy

The Internet and other information technology resources are important assets that HSD can use to gather information to improve external and internal communications and increase business efficiencies. To encourage effective and appropriate use of the state's IT resources, the following policies are in effect:

A. HSD staff shall sign and date a statement indicating they have received and read this policy.

B. HSD shall keep the staff member's signed statement on file throughout the tenure of the staff member.

C. Staff shall have no expectations of privacy with respect to state IT resource usage. HSD may install software and/or hardware to monitor and record all IT resources usage, including email and Web site visits. HSD may record or inspect any and all files stored on the assigned computing device, e.g., laptop, desktop or mobile device. These techniques may be used with the authorization of the HSD Chief Information Officer (CIO), the HSD Secretary or designate, the HSD Information Technology Division (ITD) Security Officer, the Office of Human Resources (OHR) Director, or the HSD Inspector General as part of an official investigation. Information derived from such monitoring or recording may be used in an administrative, personnel, or criminal inquiry. Illegal activity involving state IT resource usage may be referred to the appropriate authorities for prosecution.

D. Staff shall utilize state IT resources solely for state business purposes (except as described below) 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, harassment, hostile work environment, data security, and confidentiality apply to staff use of IT resources. Staff must also comply with laws governing political speech.

E. Staff shall follow all procedures regarding password security including sharing, displaying, or revealing passwords. All passwords are to be treated as sensitive, confidential HSD information.

F. Staff shall follow all IT Security and Privacy Procedures and Regulations

including protection of Personally Identifiable Information (PII), Protected Health Information (PHI), and Federal Tax Information (FTI).

G. Staff shall adhere to mandatory requirements for Information Technology training and follow all content contained within the trainings regarding computer access including computer and laptop security, password security, email security, and computer virus avoidance.

043.5.4 Prohibited Use of State IT Resources

A. Staff shall not use any state IT resources for anything other than official state business unless otherwise specifically allowed by their immediate supervisor and bureau chief/county director or another authority designated by HSD Office of the Secretary. Personal use of the state's IT resources shall be permitted only in accordance with Section 043.5.5 of this policy.

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.

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, social media sites, or chat rooms, will be subject to sanctions as outlined in existing policies and procedures associated with unauthorized release of such information.

3. Staff shall save all HSD information only on an approved, encrypted removable media device.

4. Staff shall encrypt confidential data while at rest, in use, and in transit. For example, saving confidential data to a hard drive or emailing confidential data.

5. Staff shall report suspected security incidents to the immediate supervisor and the Information Security Officer upon discovery of the incident.

6. Staff shall respect copyrights, software, licensing rules, property rights and privacy agreements.

7. Staff shall not download software, including freeware, open-source, and shareware, unless it is required to complete their job responsibilities and they have prior supervisory and ITD approval.

8. Staff shall not use State equipment to download or distribute pirated software or data, including music or video files.

9. Staff shall not use State IT resources to deliberately propagate any malicious code.

10. 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.

11. 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 ITD Chief Information Officer or the ITD Security Officer.

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

    a. Where the display or use of sexually explicit or extremist materials falls within legitimate job responsibilities, the HSD Secretary or designee may exempt a staff member in writing from the requirements. HSD shall keep the letter on file throughout the tenure of the staff member.

    b. 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.

13. Staff is 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.

14. 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.

15. 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.

043.5.5 Personal Use of the Internet

A. Occasional and incidental personal use of the state's IT resources and Internet

access is allowed subject to limitations.

1. Personal use of the Internet is prohibited if:

   a. it materially interferes with the use of IT resources by the state, e.g, downloading or streaming of internet video files that consume excessive internet bandwidth and slow down the work of others on the state network; or opening a malicious website which could make the computer vulnerable to a damaging virus or malware infection, with potential to infect other computers on the HSD network; or

   b. such use burdens the state with additional costs, e.g., downloading an application on a smartphone, or the associated administrative cost to repair, disinfect, and otherwise clean up state resources from the negative effects of viruses and malware often attached to infected freeware and web sites; or

   c. such excessive use interferes with the staff member's employment duties or other obligations to the state; or

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

043.5.6 References

HSD Code of Conduct
Governor Susana Martinez Code of Conduct Adopted April 26, 2011, Section 4. Use of State Information Technology Resources
State Security Rule (Title 1 General Government Administrative, Chapter 12 Information Technology, Part 20 Information Security Operation Management)
IRS 1075 Publication
National Institute of Standards and Technology (NIST) Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations

APPROVED: DATE:

Sidonie Squier 10/27/14

SIDONIE SQUIER, Secretary