



Department of Conservation & Natural Resources

| | | | |
|---|-------------------------------------|-----------------------|-------------|
| Information Technology Policy # IT-001 | Department Computer Resource Policy | Revised 03/06/2006 | Page 1 of 6 |
|---|-------------------------------------|-----------------------|-------------|

REFERENCES:

NRS 242.011-300 – Department of Information Technology (DOIT) Services
NRS 353A.020 – Development of Procedures requirements for the Systems for Accounting and Controls
NAC 284.638-650 – Disciplinary regulations
SAM 1511.0 – DOIT approval for purchasing
SAM 2558.8 – Checklist for Internal Controls
Information Technology Policies, Standards and Procedures of the Department of Information Technology
Information Technology Security Committee Standards

PURPOSE:

To provide for effective management of the Department's computer resources and ensure that the computer resources are used in accordance with all applicable requirements.

ORGANIZATION:

This policy applies to all agencies and employees of the department.

PRIOR POLICY:

This policy supersedes all prior policies.

INTRODUCTION

The mission of the Department of Conservation and Natural Resources is to conserve, protect, manage, and enhance the state's natural resources in order to provide the highest quality of life for Nevada's citizens and visitors. Effective computer resources are critical to the Department's ability to fulfill its mission. The majority of Department staff use computers in the performance of their respective job duties. Therefore, it is imperative that the computer resources of the agency are effectively managed. These policies and procedures provide the basic framework for effective management of these important resources.

POLICY STATEMENT

The general policy objective of each agency within the Department is to contribute to the efficiency and effectiveness of the Department's programs and business processes by maintaining functional and cost-effective computer networks and providing staff with appropriate computer resources within funding received. All computer resources shall be utilized in compliance with all applicable laws, regulations and policies and procedures.

FORMS

Attached verification form to be acknowledged by all current employees, provided to new employees upon hire, with a signed copy maintained in each employee's agency personnel file.

DEFINITIONS

“Agencies” include the Director’s Office, Division of Environmental Protection, Division of Water Resources, Division of Forestry, Division of State Lands, Division of Conservation Districts, Division of State Parks, Nevada Natural Heritage Program, and Wild Horse Commission.

“Computer resources” include, but are not limited to, host computers, file servers, workstations, stand alone computers, laptops, printers, peripheral equipment (keyboards, mouse, speakers, etc), Personal Data Assistants, LCD projectors, GPS units, database applications, software, and internal or external communications networks (such as internet, commercial online services, bulletin boards and e-mail, that are accessed directly or indirectly through the Department’s computer systems).

“DCNR Information Technology Committee” is a department-level committee comprised of a minimum of one member of each agency (with DWR representing Wild Horse) to serve as a forum and vehicle for communication related to Department data management activities and issues.

“Department” means the Nevada Department of Conservation & Natural Resources (DCNR).

“Network Administrator” means the Supervisor of each agency’s Network Administration section, if applicable, or the agency staff member designated to handle network matters. Other staff authorized by the Network Administrator are designated as backup Network administrators and are authorized to perform system administration functions.

“Users” mean all DCNR employees, authorized independent contractors and other authorized persons or entities accessing or using the Department’s computer resources and services.

GENERAL POLICIES AND PROCEDURES

1. Department computer resources are to be used for conducting official Department business or other State business authorized by the Department. Computer resources are provided to Department employees to assist them in the performance of their job duties and are not intended for personal use. Similar to Department expectations that occasional personal telephone calls be brief, use of email or internet access to attend to personal matters is allowed within the following limits: only incidental amounts of time are involved and the use does not interfere with the performance of the user’s duties or result in additional expense to the State. In addition, any personal use must not affect the performance of the computer network, e.g. by download or transmission of large graphic images, video or music files, or create the appearance of impropriety, or involve a prohibited use. Prohibited uses of computer resources include: transmission, display or storage of any material that is racist, sexist, threatening, harassing, obscene or otherwise objectionable; use of computer resources for personal monetary gain; knowing transmission of destructive programs (viruses and/or self-replicating programs); distribution of political material, or chain letters; or any illegal use.
2. All information established or used in the computer resources of the Department including, but not limited to, text files, database information and email messages, is public information except that information specifically protected through law, regulation or established policy. There should be no expectation of privacy or confidentiality for personal information or e-mails kept on State computers.
3. Department and agency management has the right and the responsibility to monitor the use of computer resources. No user may establish lockout passwords or other methods or devices within the computer resources of the Department that prevents the user’s supervisor or the Network Administrator from accessing any or all files, documents and programs.

4. All users have the responsibility to use computer resources in an efficient, effective, ethical and lawful manner. Users must comply with all software licenses and copyrights and all other state and federal laws governing intellectual property. No software may be installed on or used with Department computer resources unless the software has been purchased by, licensed to, or otherwise authorized for use by the developer or provider of the software. Software that does not require such license or specific authorization by the developer or provider of the software (such as freeware or shareware available through internet or web site applications) may be installed and used only with authorization and assistance from the agency Network Administrator or network designee.
5. Department agencies shall standardize computer software to the extent practicable. Standardization will allow for better integration of information across programs. It will also allow staff transfers within agencies with minimal software retraining requirements. New software applications will be developed in Department-approved software packages. Applications that are in use at the time of the establishment of this policy will be translated to the standard software as soon as practicable.
6. Each agency with dedicated IT staff shall provide information management services in cooperation with professional staff. These services include network administration; PC maintenance and desktop support; programming and application development; database administration; website development and maintenance; GIS services and purchasing, receiving and inventory of computer resources and software. In agencies without dedicated IT staff, or limited IT staff, some or all of these services may be provided through assignments to various staff members.
7. Access to information held within the Department's computer resources shall be controlled to limit unauthorized use and/or inappropriate manipulation of information. The security procedures are established below.
8. All users are responsible for the integrity of and protection of information developed and used in their job duties.
9. Violations of this policy may result in disciplinary action in accordance with NAC 284.638-650.

SYSTEM SECURITY/ACCESS

1. Access to the Department's computer resources will be restricted to users who have authorization as evidenced through an official request by their supervisor. Each user with proper authorization will be granted a user account.
2. Users will be required to use a password to gain access to their account and will be required to change their password periodically. Users are responsible for safeguarding their system passwords. Individual passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passwords.
3. To prevent unauthorized access to a user's account, the account shall be automatically disabled after a set number of incorrect login attempts. Disabled user accounts can only be re-enabled by the agency's Network Administrator or network designee.
4. At the time any employee or contract personnel terminates his or her relationship with the Department, all computer resources and information contained therein must be returned to the respective agency. The immediate supervisor is responsible for ensuring all state information resource property in the custody of the worker is returned.

5. Supervisors must ensure that the Network Administrator or agency network designee is promptly notified of terminations. The Network Administrator or designee will then promptly terminate all system privileges of the worker.
6. In the event that staff (or a contractor of an agency) is terminated involuntarily, the Supervisor shall immediately notify the Network Administrator or agency network designee. System access capabilities must be immediately revoked by the Network Administrator or designee, including access connections, dial-up accounts, and e-mail addresses.

INVESTIGATION PROCEDURES

1. Each Information Security Officer in the Department shall establish an Investigative Log File to record access to an employee or contractor's computer for investigation of alleged inappropriate use. Access for purposes of routine maintenance, repair or upgrade shall not be recorded in the log file unless staff tasked with performing routine maintenance of computer resources discovers evidence of inappropriate use while accessing a computer. In that case, the staff person shall provide the details of the alleged inappropriate use to the Information Security Officer assigned to the agency to record in the Investigative Log File, and report the alleged inappropriate use to the Agency administrator. The Investigative Log File shall be maintained as a confidential document and shall include:
 - a. Requesters name;
 - b. Date and time access to the computer resource in question will occur or has occurred;
 - c. Date of approval of the request for investigation;
 - d. Brief explanation justifying the need for access to the computer;
 - e. Name of each person required to gain access;
 - f. Name of each person allowed to examine information obtained during access;
 - g. Name of each person authorized to archive, maintain, store, transfer, transmit or destroy information obtained during the investigation.
2. Requests for investigation of inappropriate use of computer resources by employees or contractors must be submitted in writing through recognized supervisory channels to the Agency administrator.
3. After validation of a request for investigation, the Information Security Officer assigned to the Agency will ensure that the request is included in the Investigative Log File.
4. The Information Security Officer shall personally handle or assign the task to the Network Administrator or another IT staff person to complete the investigation and file a written report of the findings.
5. The Information Security Officer shall forward the report to the appropriate Agency administrator for appropriate action.

ELECTRONIC MAIL

1. Electronic mail (e-mail) is to be used for state business related communications. Although incidental personal use is permissible within the limits prescribed by this policy, the user has no right to privacy. As a public agency, the Department's records are subject to public inspection, including electronic files and e-mail. Users should use the same care in drafting e-mail and other electronic documents as they would for any other written communication. Anything created on the computer may, and likely will, be reviewed by others.

2. Users should always logout from their computer whenever it is left unattended to prevent unauthorized persons from sending e-mail using their login name.
3. Fraudulent, harassing, embarrassing, indecent, profane, obscene, intimidating, or other unlawful material may not be sent by e-mail or other form of electronic communication or displayed on or stored on any Department computer. Anyone encountering or receiving such material should immediately report the incident to his or her supervisor.
4. Users who are not employees of the Department will not be granted access to the e-mail system except by specific authorization from a DCNR agency administrator.
5. Users should exercise care to avoid opening an e-mail, or e-mail attachment, that contains a virus. Users should delete e-mail that appears suspicious and is from an individual or organization unknown to the user.

SOFTWARE USE and ASSET MANAGEMENT

1. The Department is committed to complying with copyright laws and regulations, intellectual property rights of software developers and software license agreements. No software may be installed on or used with Department computer resources unless the software has been properly licensed to the Department or has been otherwise authorized for use by the developer or provider of the software.
2. Copyrighted software may not be duplicated, with the exception of archival or back-up purposes and other uses specifically authorized in the license agreement. Software that is licensed to the Department may not be loaned or distributed to others in violation of license agreements.
3. All requests for purchase of software and software upgrades shall be approved by the proper agency authorities and submitted to the Network Administrator or network designee for procurement. Purchased software shall be received by the Network Administrator or network designee and installed by IT staff after product and licensing information has been entered in the software recordkeeping system.
4. In order to maintain an accurate inventory, the Network Administrators or network designee shall be provided with evidence of proper licensing (license agreement or original media) regarding software received through means other than the purchasing process.
5. Agency IT staff will conduct periodic auditing, using a software-auditing tool, to compare inventory records with installed software and ensure compliance with license agreements. Reports of audit findings shall be provided to agency Administrators and the Department Director.

RESPONSIBILITIES

1. All users are responsible for:
 - a. Utilizing the Department computer resources in accordance with these policies and procedures and any other applicable requirements.
 - b. Ensuring that access to all documents, software, files or other information is always available to his/her supervisor and to the Network Administrator.
 - c. Ensuring the accuracy and integrity of all data and information that the user inputs or modifies through the use of Department computer resources.
 - d. Storing Department data and any important documents on a LAN file server if available.
 - e. Acquiring the competency needed to effectively utilize the computer resources provided to them by the Department.

DISTRIBUTION

1. DCNR Agencies (and all employees):
 - a. Director's Office
 - b. Division of Environmental Proteciton
 - c. Division of Water Resources
 - d. Division of Forestry
 - e. Division of State Parks
 - f. Division of State Lands / Conservation Districts
 - g. Nevada Natural Heritage Program
 - h. Wild Horse Commission

| | |
|--|-----------------------------|
| <hr/> Approved By (DCNR Director) | <hr/> Effective Date |
|--|-----------------------------|

Department of Conservation and Natural Resources
Computer Resource Policy Verification
Information Technology Policy #IT-001

Employee Name:

Agency ID:

Employee ID:

Division:

I have read and understand the **Department Computer Resource Policy [*Information Technology Policy #IT-001*]** dated 03/06/2006, which delineates my responsibilities as a State/DCNR Employee regarding use of the computers, the Internet and other electronic communications channels, and agree to be bound by its content.

I am aware that I may be subject to disciplinary action of a warning, suspension or dismissal, and/ or appropriate legal action for any proven infringement or violation of Information Technology Policy #IT-001.

Employee Signature:

Supervisor Signature:

Date:

Date: