

**NEVADA DEPARTMENT OF CORRECTIONS
ADMINISTRATIVE REGULATION
142**

ACCEPTABLE USES OF INFORMATION TECHNOLOGY

Supersedes: AR 142 (06.01.05)

Effective date: 11/14/08

AUTHORITY: NRS 209.131; NRS Chapters 242 and 281

RESPONSIBILITY

All Department staff, vendors, contract employees and volunteers who operate information technology systems in the Department are responsible for compliance with the requirements of this AR.

142.01 USER ACCOUNT AND PASSWORD POLICY

1. Each computer or communications system user account, username, or user-ID must uniquely identify only one user.
 - A. Shared or group user-IDs and passwords are prohibited.
 - B. The MIS manager must pre-approve any exception to this standard (i.e. training).
2. No user shall disclose a password to any other person, and the user must change their password promptly if it has been compromised or is suspected of having been compromised.
 - A. A user may disclose their password only to a department MIS staff member and then only for the purpose of providing support on a help ticket.
 - B. MIS recommends that users change their password after the completion of a help ticket.
 - C. No user shall access any system or device using any user ID or password not assigned specifically to that user.
 - D. The display or printing of passwords must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or recover them.
3. Vendor supplied default passwords should be changed before any IT device or system is used for department business or connected to a department network.
4. System administrators must immediately change every password on a system if password file integrity is, or is suspected of having been, compromised.
5. Passwords are not authorized to be used with a Department information system on any other information systems that will be used to access the Internet.

- A. The same password will not be used for both local and remote Internet access systems.
 - B. Passwords should not be so obvious that others could easily guess them.
6. The MIS manager must determine regular intervals for changing all user passwords.
 7. The number of consecutive attempts to enter a password will be limited to three attempts, after which the involved user name shall be disabled until verified and reset by a systems administrator.
 8. Passwords cannot be entered or changed in a computer system for authentication and authorization purposes unless the representative for the system granting access has taken reasonable steps to positively identify the requester.
 9. All requests for entry or change of passwords must be confirmed by either:
 - A. Direct contact or voice recognition; or
 - B. Confirmation from the employee's immediate supervisor; **and**
 - C. Knowledge of predefined key words or phrases by the requester for password changes; or
 - D. Callback initiated by MIS through the employee's immediate supervisor.
 10. Upon termination of a user's employment with the Department, or upon transfer to another position or institution, an employee's immediate supervisor should immediately inform the help desk of the change in access requirements.
 - A. Supervisors assume responsibility for use or misuse of a former employee's user account or password that is not deactivated.
 - B. The MIS Division will use Personnel/IFS records as the authoritative source for information regarding an individual's employment status.

142.2 ELECTRONIC MAIL PROCEDURES

1. Personal use of e-mail on the state system is a privilege and not a right.
 - A. This privilege may be revoked at any time.
 - B. Abuse of the privilege may result in disciplinary action.
 - C. All e-mail sent or received via the Department's systems may be recorded and stored along with the source and destination.
 - D. Personal e-mail should not impede the conduct of department business.
 - E. Staff shall not use department systems to subscribe to any mailing list or mail services strictly for personal use without approval of the MIS Manager.
 - F. Personal e-mail should not cause the Department to incur a direct cost in addition to the general overhead of e-mail.
2. Personal use of State e-mail systems on breaks and lunch hours is acceptable.

3. E-mail should not be used for outside business activities or monetary interest or gain.
4. Staff has no right to privacy regarding e-mail usage on the Department's systems; recorded e-mail messages on the Department systems are the property of the Department.
5. Supervisors who suspect inappropriate or illegal use of the State e-mail system should request an investigation through the Inspector General's Office.
6. When sending an e-mail of a personal nature on the state system, there is a danger of the staff's words being interpreted as official department policy or opinion. Therefore, when an employee sends a personal e-mail on the state system, especially if the content of the e-mail could be interpreted as official Department statements, the employee should use the following disclaimer at the end of the message. "This e-mail contains the thoughts and opinions of (staff member's name) and does not represent official Department of Corrections' policy."
7. Accessing, posting or sharing any racist, sexist, threatening, obscene or otherwise objectionable material either visually, textually, or audibly, is strictly prohibited.
8. Staff should not intentionally use the Internet facilities or e-mail to disable, impair, or overload performance of any computer system or network.
9. Staff should not intentionally use the Internet facilities or e-mail to circumvent any system intended to protect the privacy or security of the system or other net users.

142.03 INTERNET PROCEDURES

1. Users should not represent themselves as other persons in e-mail without the consent of those other persons and when such proxy representation is defined as a job requirement.
 - A. Proxy representation must occur through proper setup of an e-mail system, via a request to the MIS Help Desk.
 - B. Under no circumstances shall users divulge a password to allow such access.
2. Internet services are provided by the Department to:
 - A. Support open communications and exchange of information;
 - B. Allow the opportunity for collaboration in government related work.
3. The Department encourages the limited use of electronic communications by its staff.
 - A. The user is responsible to inquire as to acceptable and unacceptable uses prior to use.

- B. Staff should use the Department provided Internet services for government related activities and not for outside business activities.
4. Internet should not be used for outside business activities or monetary interest or gain.
 - A. Staff has no right to privacy with regard to Internet usage on the Department's systems.
 - B. Management has a right to review staff usage patterns and take action to assure that the Department's Internet resources are devoted to maintaining a high level of productivity.
 5. Supervisors who suspect inappropriate or illegal use of the State Internet should request an investigation through the Inspector General's Office.
 6. Staff should know and follow the generally accepted etiquette of the Internet including:
 - A. Use civil forms of communication;
 - B. Respect the privacy of others;
 - C. Respect for legal protection provided by copyright and licensed programs and data;
 - D. Respect the privileges of other users.
 - E. Respect the integrity of computing systems connected to the Internet;
 - F. Staff shall avoid use of the Internet that reflects poorly on the Department or state government;
 - G. Remember that existing and evolving rules, regulations, and guidelines on ethical behavior of staff and the appropriate use of government resources apply to the use of electronic communication systems supplied by the Department.
 7. If at some future point, an employee no longer needs Internet access, the employee should notify the department manager or supervisor, or designee of that circumstance.
 8. Acceptable uses of the Internet include:
 - A. Communication and information exchange directly related to the mission, charter, or work tasks of the Department;
 - B. Communication and exchange for professional development, to maintain currency of training or education, or to discuss issues related to the user's department activities;
 - C. Use in applying for or administering grants or contracts for the department's research or programs;
 - D. Announcement of new state laws, procedures, policies, rules, services, programs, information, or activities;
 - E. Any other governmental administrative communications not requiring a high level of security;

- F. Communications incidental to otherwise acceptable use, except for illegal or specifically unacceptable usage;
 - G. Used for advisory, standards, research, analysis, and professional society activities related to the user's department work tasks and duties.
9. Unacceptable uses of the Internet include:
- A. Use of the Internet for any purpose which violates a U.S. or Nevada law (NRS Chapters 205, 239, and 603, code or policies, administrative regulations, standards and procedures). Use for any profit-making activities unless specific to the charter, mission, or duties of the department.
 - B. Use for purposes not directly related to the mission, charter, or work task of the Department during normal business hours.
 - C. Use for private business including commercial advertising.
 - D. Use for access to or distribution of indecent or obscene material or child pornography;
 - E. Use for access to or distribution of computer games that have no bearing on the Department's mission, other than those specifically related to Department training or educational activities.
 - F. Use of Internet services so as to interfere with, or disrupt network users, services, or equipment;
 - G. Use the Internet services to seek information, distribute information, obtain copies of, or modify files and other data that is private, confidential or not open to public inspection, or release such information as set forth in NRS 239 or departmental administrative regulations, unless specifically authorized to do so once the legal conditions for release are satisfied;
 - H. Users intentionally copying any software, electronic file, program, or data without a prior, good faith determination that such copying is in fact permissible;
 - I. Users misrepresenting themselves as other persons on the Internet, without the express consent of those persons;
 - J. Use of Internet services to develop programs designed to harass other users, or infiltrate a computer or computing system, and or damage or alter the software components of the same, such as viruses;
 - K. Use for fund-raising or public relations activities not specifically related to Department activities approved in writing through the chain of command and;
 - L. Use of the Internet for any type of gambling;
 - M. Installation of any software over the Internet without approval by the MIS manager

142.04 INSPECTION OF COMPUTERS

1. Staff who become aware of the inappropriate use of a computer belonging to the State or located within an institution or facility of the Department should report this circumstance to the IG.

- A. Staff whose computer is to be inspected should receive written notice of this inspection prior to or no later than 48 hours after the conduct of the inspection.
- B. Notice of inspection is not required if the inspection is an element of a criminal investigation by the IG or other law enforcement agencies.
- C. MIS staff performing maintenance on computers and systems is not required to give notice of the maintenance actions prior to accessing a computer.

142.05 MISCELLANEOUS GUIDELINES

1. Any software or files downloaded should be virus-checked prior to use.
2. Contractors and other non-State staff may be granted access to Department provided Internet services at the discretion of the Department.
 - A. Acceptable use by contractors and other non-State staff working for the Department is the responsibility of the contracting division.
 - B. The contracting division should provide contractors who use the Department Internet services with information, guidelines, and policy on Internet usage.
 - C. All contractors should sign a memorandum prior to usage acknowledging a complete and thorough understanding of Department regulations governing computer usage prior to passwords and accounts being assigned.
3. Temporary accounts and addresses should be assigned by the MIS Help Desk after a receipt of a request for service.
 - A. This account should be flagged for deletion after 45 days as a security measure.
 - B. The contracting division may request an extension after 30 days if necessary to ensure uninterrupted access for contractors.
 - C. Temporary addresses must be under strict supervision with appropriate audit techniques implemented.
 - D. Temporary addresses must be deleted immediately upon non-State employees' or contractors' departure, or the end of the project requiring access to the Internet.
4. A reasonable attempt should be made to complete the log off, or other termination procedure, when finished using a remote Internet access to system or resource.
5. Unencrypted electronic-mail sent or received from outside any Department or on the Internet cannot be expected to be secure. Use discretion when sending documents over the Internet that is confidential in nature.
6. Users contemplating file transfers over 10MB per transport, or interactive video activities, should schedule these activities after business hours, or early or late in the day.

142.06 APPLICABILITY

1. This regulation requires the development of Operational Procedures within MIS and the Office of Inspector General.
2. This regulation does not require an audit.

Howard Skolnik, Director

Date