

**NEVADA DEPARTMENT OF CORRECTIONS  
ADMINISTRATIVE REGULATION  
141**

**INFORMATION TECHNOLOGY STANDARDS, CONTROLS AND  
SECURITY; ACCEPTABLE USES OF INFORMATION TECHNOLOGY**

**Supersedes:** AR 141 (03/19/13); and AR 141 (Temporary, 11/25/13)  
**Effective date:** 12/17/13

**AUTHORITY:** NRS Chapter 209.131; NRS Chapter 242 and 281

**RESPONSIBILITY**

1. The Management Information Systems (MIS) Manager is responsible for the approval of information technology (IT) and telecommunications activities and is the single point of contact between the Department of Corrections and the Enterprise Information Technology Services (EITS).
2. All Department staff, contract employees and volunteers, as well as all other persons who are allowed the privilege of accessing or using information technology (IT) or telecommunication systems within a secure environment or directly connected to Department IT resources, are responsible to have knowledge of, and comply with, this regulation.
3. 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 Administrative Regulation.

**141.01 REGULATING THE USE OF EQUIPMENT AND INFORMATION**

1. The use of information technology (IT) or telecommunications for any purpose within the Department should be strictly regulated to ensure:
  - A. That information may be shared throughout the Department using standardized tools, including hardware, software, data communication protocols, and operational procedures;
  - B. The protection, the security and integrity of information;
  - C. The coordinated and economical procurement of equipment;
  - D. The prevention of the unnecessary proliferation of equipment; and
  - E. The prevention of the unauthorized relocation of existing equipment.

2. Any unauthorized use of IT or telecommunication devices, software, or services may result in loss of access to such devices or systems, removal of systems, disciplinary action, and/or criminal prosecution.

3. The use of IT and telecommunications is a privilege and not a right.

4. All Department staff, contract employees and volunteers, as well as all other persons who are allowed the privilege of accessing or using information technology (IT) or telecommunication systems within a secure environment or directly connected to Department IT resources, must sign the Information Technology and Telecommunications Device Agreement and Acknowledgment, DOC Form 003.

A. Failure to sign this agreement could result in revocation or denial of access to Department information systems.

#### **141.02 COMMERCIAL SOFTWARE**

1. A legal license must be purchased for each user, computer or processor, as specified in the vendor's license agreement.

2. All questions regarding a proprietary nature of commercial software should be directed to the Chief, IT Manager.

3. The original media for each piece of commercial software will be maintained by MIS in a central library.

4. All license or registration certificates, purchase agreements or other similar documentation governing the use of commercial software will be maintained by MIS in a central library.

5. The use of such software other than in strict accordance with license, lease or registration agreements is forbidden.

A. Violators may be subject to disciplinary action, criminal prosecution, or civil enforcement action.

#### **141.03 OPEN SOURCE SOFTWARE (OSS)**

1. The Chief, IT Manager must approve any open source software before use.

A. Open Source Software (OSS) is software, which may or may not be provided free of charge, for which the underlying programming code is available for anyone to read it, make changes to it, and build new versions of the software incorporating their changes.

2. The use of any open source software must be in accordance with the terms of any licensing agreements governing its use.

#### **141.04 FREE OR PUBLIC DOMAIN SOFTWARE**

1. The Chief, IT Manager must approve any free or public domain software before use.
  - A. Free software, also known as freeware, or public domain software, is any piece of software that is available for use without any payment or other compensation to its author.
2. The use of any free software must be in accordance with the terms of any licensing agreements governing its use.

#### **141.05 USE OF DEPARTMENT RESOURCES ON NON-STATE EQUIPMENT**

1. All IT and telecommunication resources purchased or used by the Department, including any software licensed to the Department or that resides in the Department's computers, is the property of the Department and the State of Nevada.
  - A. Open source software modified or written by MIS staff in the course of their duties may be freely shared on the Internet, in accordance with the General Public License (GPL) or other license governing the use of such software.
2. The Chief, IT Manager must pre-approve, in writing, the removal of any device or any licensed or proprietary software from the Department, allowing employees to work on any non-Department owned equipment.
  - A. An inventory will be maintained by MIS of any equipment or software authorized for use outside the Department's systems.
3. As is the case with all public property, Department equipment and software may not be used for any purpose other than that which is necessary for the proper administration of the duties, responsibilities, and business of the Department under the laws of the State of Nevada.
4. Use of Departmental IT or telecommunication resources in a matter not related to the conduct of the Department's business or for a private purpose for which the employee may gain personal benefit is a violation of Nevada law, and will be subject to investigation, disciplinary procedures and/or criminal prosecution.

#### **141.06 PROPRIETARY INFORMATION**

1. All data and information which reside in the Department's computers and systems are the property of the Department and the State of Nevada.
2. Department information may not be used for any purpose other than that which is necessary for the proper administration of the duties, responsibilities, and business of the Department under the laws of the State of Nevada.
3. Use of departmental information in a matter not related to the conduct of the Department's business is a violation of Nevada law.

4. As is the case with all public property, conversion of proprietary information for a private purpose for which the employee may gain personal benefit is a violation of Nevada law.

5. There may be specific restrictions which also apply to the use of Department information for legitimate business purposes.

A. Certain types of personal and inmate information may be restricted because they are confidential or of a sensitive nature.

6. The electronic transmission of any proprietary or confidential information must comply with all applicable federal, state and local laws, and any State or Department policies or procedures regarding privacy and/or encryption of such information in transit.

7. Physical transmission of devices containing NDOC information must comply with all applicable federal, state and local laws, and any State or Department policies or procedures regarding privacy and/or encryption of such information.

A. If the contents of the device are unknown, they must be treated as if they contain proprietary or confidential information.

B. Devices that will be in the possession of a third party, must have the data removed prior to shipment by a process meeting applicable federal, state and local laws, and any State or Department policies or procedures regarding data removal.

#### **141.07 PROCUREMENT AUTHORITY**

1. The Chief, IT Manager must pre-approve all information technology and telecommunications related purchases.

A. This requirement applies to all divisions, institutions, and facilities of the Department regardless of the source of funding.

B. This requirement applies to any electrical or electronic device, software, service or related item that will connect to, or has the potential to connect to, or will interact with, any Department computer, network, phone line, etc., or can in any way be construed as information technology.

C. MIS will maintain operational procedures listing examples of information technology and telecommunications devices covered by this requirement, including guidance on the selection of such devices for use within the Department.

2. The Chief, IT Manager should consider budgetary authority, compliance with regulations, and whether the purchase is consistent with the direction adopted by the Department.

#### **141.08 DONATED/SURPLUS EQUIPMENT**

1. The Chief, IT Manager must pre-approve, in writing, all donated or surplus equipment and software.

2. The Chief, IT Manager must pre-approve any personal hardware and software used in the Department or on department computers.

3. An IT or telecommunication device, system, or software that is brought into any department location without approval by the Chief, IT Manager, or Director if required, will be considered contraband, and will be subject to removal and/or disciplinary or criminal action as appropriate.

#### **141.09 INVENTORY**

1. The Chief, IT Manager is responsible for preparing and maintaining an inventory of all Department hardware and software and telecommunication devices.

2. An inventory will be established and will be updated on an annual basis, or as needed. Specifics of the inventory contents should be included in operational procedures.

3. Copies of this inventory should be distributed to all appointing authorities who use this technology.

4. The Chief, IT Manager must approve the location or relocation of any IT device, system, software or telecommunication device that is owned, maintained or operated by the Department or will be used in any Department location.

5. Relocation without approval may result in loss of access to systems or removal of systems, and/or disciplinary action against the user or prosecution under criminal statutes.

#### **141.10 ACCESS TO STATE RESOURCES**

1. The Warden, Facility Manager or Division Head will identify authorized staff to access State owned equipment, software, systems, networks, services and other resources.

2. Access to information technology and telecommunication resources or services will be requested by the Warden, Facility Manager or Division head through the MIS Help Desk.

3. Access to information technology and telecommunication resources and services is granted to authorized individuals only; Any user name, password, security device or other form of electronic identification or authorization given to an individual for access to IT or telecommunication resources cannot be shared or delegated to any other individual.

A. Exceptions to this requirement require written pre-approval by the Chief, IT Manager and must be necessary to a specific job function.

4. Access to another user's resources and information is allowed as required by job duties and by use of a system proxy function or permission setting only; Such access functions with a user logging in with their own user name, and not by using another person's account or password.

5. Changes in position, title or duty station will result in current access being terminated, and the Warden or Manager must request new access for that individual through the MIS Help Desk.

6. The use of another individual's user name, authorization, access code, security device, etc. to access any IT or telecommunication resource, or the unauthorized access of another user's resources or information, will result in loss of access to such resources, and/or disciplinary action against the user or prosecution under criminal statutes.

#### **141.11 USER ACCOUNT AND PASSWORD POLICY**

1. Each information technology system user account, username or user-ID must uniquely identify only one user.

A. Shared or group user-IDs and passwords are prohibited.

B. Any exception to this standard (i.e. training) requires documented approval by the Chief, IT Manager.

2. No user shall disclose a password to any other person and must change the 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 Management Information Systems (MIS) staff member and then only for the purpose of providing support on a help ticket.

B. If a password is disclosed to MIS in the course of resolving a help ticket, then users must change their password after the completion of the help ticket.

C. No user shall access any system or device using any user ID or password not assigned specifically to that person.

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. The same password will not be used for both local and remote systems accessed via the Internet. For example: if you have a VPN or use Terminal Services, that password should not be the same as your NDOC passwords.

6. Passwords should not be so obvious that others could easily guess them.

7. All user passwords must be changed at regular intervals determined by the Chief, IT Manager.

8. 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 system administrator.
9. 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.
10. All requests for entry or change of passwords must be confirmed by either:
  - A. Direct contact or voice recognition; or
  - B. Confirmation from the employees 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.
11. Upon termination of an employee's employment with the Department, or upon transfer to another position or institution, the appointing authority should immediately inform the help desk of the change in access requirements.
  - A. The Appointing Authority is responsible 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 employee's employment status.
12. After a defined period of inactivity (specified in operational procedures for each system), all systems requiring authorization will automatically end or secure the user session, requiring the user to re-authenticate to unlock the system or restore their session.

#### **141.12 ELECTRONIC MAIL PROCEDURES**

1. 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.
2. Staff has no right to privacy with regard to e-mail usage on the Department's systems.
  - A. All e-mail sent or received via the Department's systems may be recorded and stored along with the source and destination.
  - B. Recorded e-mail messages on the Department systems are the property of the Department.

3. Use of e-mail should not impede the conduct of department business.
  - A. Staff shall not use department systems to subscribe to any mailing list, mail services or to access any social media networks without approval of the Chief, IT Manager.
  - B. To avoid unwanted email (spam), staff should be cautious about using their Departmental email address on any website or system where it is not essential to their job function.
4. E-mail should not be used for outside business activities or monetary interest or gain.
5. Supervisors who suspect inappropriate or illegal use of the State e-mail system should request an investigation through their chain of command.
6. When sending an e-mail message from a State system, there is a danger of an individual's words being interpreted as official Department policy or opinion, even when they are not authorized to speak on behalf of the Department. Therefore, when employees send personal e-mails 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 e-mail to disable, impair, or overload performance of any computer system or network.
9. Staff should not intentionally use e-mail to circumvent any system intended to protect the privacy or security of the system or other users.
10. 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
  - B. Under no circumstances shall users divulge a password to allow such access.
11. Staff should know and follow the generally accepted etiquette of e-mail including:
  - A. Use civil forms of communication;
  - B. Respect the privacy of others;
  - C. Respect the privileges of other users.



D. Staff shall avoid use of the e-mail that reflects poorly on the Department or state government;

E. 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.

F. The following statement will be added to all outgoing emails generated on the NDOC email system. **“This preceding e-mail message and accompanying documents are covered by the Electronic Communications Privacy Act, 18 U.S.C. SS 2510-2521, and contains information intended for the specific individual(s) only or constitute non-public information. This information may be confidential. If you are not the intended recipient you are hereby notified that you have received this document in error and that any review, dissemination, copying, or the taking of any action based on the contents of this information is strictly prohibited. If you have received this communication in error, please notify me immediately by E-mail, and delete the original message. Use, dissemination, distribution or reproduction of this message by unintended recipients is not authorized and may be unlawful.”**

G. No other graphics, logos, designs, or sayings other than the sender’s contact information should be included, along with the footer information listed in section 141.12.F above.

#### **141.13 INTERNET PROCEDURES**

1. Use of Internet access 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.
2. Staff has no right to privacy with regard to Internet usage on the Department’s systems.
  - A. All Internet usage via the Department’s systems may be recorded and stored along with the employee’s name, date, and other related information.
  - B. Recorded Internet usage logs on the Department systems are the property of the Department.
3. 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.
  - A. Use of Internet should not impede the conduct of department business.
  - B. If at some future point, Internet access is no longer necessary, an employee should notify their supervisor of that circumstance.
  - C. Supervisors who suspect inappropriate or illegal use of the State Internet should request an investigation through their chain of command.

4. 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.
5. 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.
6. 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).
  - 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, adult entertainment/pornography, 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. Intentionally use Internet facilities to disable, impair, or overload performance of any computer system or network.

G. Intentionally use Internet facilities to circumvent any system intended to protect the privacy or security of the system or other users, including the use of proxy services, or any other means, to bypass content filtering.

H. 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;

I. Users intentionally copying any software, electronic file, program, or data without a prior, good faith determination that such copying is in fact permissible;

J. Users misrepresenting themselves as other persons on the Internet, without the express consent of those persons;

K. 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;

L. Use for fund-raising or public relations activities not specifically related to Department activities approved in writing through the chain of command and;

M. Use of the Internet for any type of gambling;

N. Installation of any software over the Internet without approval by the Chief, IT Manager.

O. Use for any profit-making activities, online auctions, online shopping, etc., unless specific to the charter, mission, or duties of the Department.

P. Access any kind of non-business related chat service, social media networks or functions.

Q. Use any kind of voice over Internet Protocol (IP) service not specifically authorized by the Chief, IT Manager.

#### **141.14 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 through their chain of command.

A. Staff whose computer is 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 initiated by the Director.

C. Notice of inspection is not required if the inspection is an element of a documented and numbered IG investigations and/or review.

D. Notice of inspection is not required if the inspection is an element of a criminal and/or administrative investigation by the IG or other law enforcement agencies.

E. Inspection of computers will be in accordance with NRS 281.195

F. The discovery of inappropriate usage by any staff member in the normal course of their duties or during routine system maintenance is not considered an inspection.

2. All computers entering a correctional institution/facility must be physically inspected and/or approved by MIS before being allowed into the Institution/Facility.

3. Personal or non-approved information technology equipment found within an Institution/Facility will be considered contraband.

#### **141.15 MISCELLANEOUS GUIDELINES**

1. Any software or files downloaded should be virus-checked prior to use. For example, if you connect a device to the computer and it asks if you want to virus scan it, you must answer Yes.

2. Contractors and other non-State staff may be granted access to Department provided information technology resources with the approval of MIS.

A. Acceptable use by contractors and other non-State staff working for the Department is the responsibility of the contracting or supervising division.

B. The contracting division should provide contractors who use the Department information technology resources with information, guidelines, and policy on Internet usage.

C. All non-State staff should sign the Information Technology Agreement (DOC Form 1046) prior to usage, acknowledging a complete and thorough understanding of Department regulations governing information technology usage. The signed form must be received by MIS prior to passwords and accounts being assigned.

D. The Help Desk will track all contractor and non-state staff accounts and assign a DOC-generated ID number to identify the account.

E. Temporary accounts will be assigned a termination or expiration date, so that the Help Desk may follow up to ensure they are disabled or deleted at the appropriate time.

3. Users must complete the log off or other termination procedure when finished using any IT resource or system.

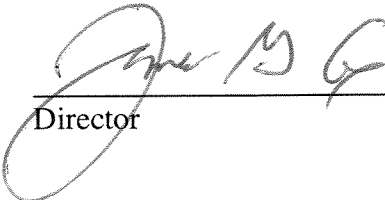
4. Unencrypted electronic-mail sent or received from outside any Department or on the Internet cannot be expected to be secure. All staff must comply with NRS 597.970 regarding the


encryption of personally identifiable information, as well as any other confidential information, when sending or receiving messages outside of NDOC's email system.

5. 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.

**APPLICABILITY**

- 1. This regulation may require the development of Operational procedures within MIS or at an institution.
- 2. This regulation requires an audit.

  
\_\_\_\_\_  
Director

  
\_\_\_\_\_  
Date