



NEVADA DEPARTMENT OF CORRECTIONS
ADMINISTRATIVE REGULATION

**OFFENDER ACCESS TO INFORMATION TECHNOLOGY
ADMINISTRATIVE REGULATION – 143**

SUPERSEDES: AR 143 (11/14/08); AR 143 (Temporary 6/13/16); AR 143 (08/16/16)

EFFECTIVE DATE: September 30, 2022, TEMPORARY EDITION

AUTHORITY: NRS 209.417

RESPONSIBILITY

The Director of the Nevada Department of Corrections (NDOC and Department), is responsible for the implementation of this Administrative Regulation (AR).

All staff ~~should be~~ responsible for being familiar with the requirements of this regulation and enforcing its requirements. Failure of a staff member to properly manage offender access to information technology may result in disciplinary action against the staff member.

143.01 ~~RESTRICTIONS ON OFFENDER USE OF DEPARTMENT COMPUTER EQUIPMENT IS GENERALLY RESTRICTED~~

1. Except as otherwise provided in section 143.02, No offender shall ~~not~~ be allowed to work ~~on or~~ with any computer, computer system, or information system ~~that is connected to in any way to any~~ external network, ~~or~~ that is equipped with a modem, network card, or similar device which would permit data ~~communications or other~~ communications of any type with a person or device outside a Department institution or facility.
2. Internal networks shall not be connected in any way to any communications device or technology that will allow communications outside of the building or the work location defined for such a network.
4. The MIS-Information Technology (IT) manager must pre-approve all internal, offender networks before installation and operation. The responsible staff member must fully document the need to the MIS-IT manager.
 - A. Such networks must be staff-designed and must remain under management and control of staff.

-
- B. No networks may be designed and/or controlled by offenders.
4. It is the responsibility of authorized staff to ensure the security of the institution and computer network is not breached. This is to be accomplished through staff monitoring and presence during the operation of the computer lab. All offenders entering the computer lab will be identified by call-out and/or offender pass. Those offenders not on the call-out or pass list shall be denied access.
- A. All offenders will be identified prior to entering the computer lab by staff conducting the class and directed to sign-in.
- B. Any suspicious activity observed or suspected by the instructor or any NDOC staff may be cause for the removal of an offender from the program.
- C. A correctional officer or NDOC staff shall periodically conduct unannounced and random checks.
- D. There will be a detailed schedule of lab operations.
- E. Changes to an information system must be fully documented and authorized and must be accepted in a controlled manner.
- F. IT will make sure anti-virus software is deployed on all computer systems and ensure that all anti-virus software is current, actively running, and generating audit logs.
- G. Only IT staff ~~from~~are unauthorized to complete software installations on any Department computers. All others are prohibited.
- A. ~~Prohibit anyone except~~Only IT staff ~~from~~are unauthorized to perform the copying of sensitive data and secure data backups. All others are prohibited.
- ~~B-H.~~
- I. Information systems must be configured appropriately to record all critical activities such as login/logout and administrative changes. IT will provide the minimal necessary access that is required.
- J. URLs will be reviewed and approved by program/education staff.
- K. Software/hardware changes will be made by IT staff.
5. No offender may write or modify any computer software that is owned, leased, or used by the state, or utilize such software to collect or organize personal or state proprietary data.

-
6. An offender shall not be called upon under any circumstances to provide technical assistance or otherwise assist staff with the resolution or attempted resolution of any computer problems, computer system, or information system problems.
 7. Offenders may not have any type of secret file or password-protected file on any computer.
 - A. The offender shall immediately be terminated from their assignment if secret or password-protected files are discovered.
 - B. The offender shall no longer have any access to any information systems during the remainder of their incarceration.
 8. This regulation also applies to all offenders working in a community setting.

143.02 PERMISSIBLE OFFENDER COMPUTER EQUIPMENT AND ACTIVITIES

1. An offender may work with a computer that utilizes a formal program of education or vocational training, ~~or legal research,~~ or approved programming by Program Review Committee on a closed network.
2. An offender may utilize a standalone, state computer for structured assignments under the supervision of a staff member.
3. Offenders ~~that are classified for programming, with prior approval by the Director or assigned designee, may access a computer with as Community Trustee or assigned to Casa Grande Transitional Housing or Northern Nevada Transitional Housing may, with prior approval, access a computer with~~ internet capabilities for the purpose of:
 - A. Obtaining educational or vocational assessments, training, provision of medical services, judicial proceedings, or certificates that are approved by the Department; Searching or applying for employment.
 - B. Searching for or applying for employment; Participating in approved vocational or educational training.
 - C. Searching for or applying for applicable state or government benefit programs; Completing approved vocational or educational tasks.
 - D. Performing essential job functions; Completing assigned community employer job duties and assignments.
 - E. Participating in a video conference pursuant to a valid Court Order; or
 - A-F. Providing medical services for offenders via a remote tele-medicine platform.

-
4. Offenders ~~that are~~ classified as Community ~~Trustee-Trusty~~ or assigned to Casa Grande Transitional ~~HousinHousingg -or of~~ Northern Nevada Transitional Housing may, with prior approval, use a telecommunication device if it is required by a community employer to complete essential job functions.
 5. ~~Except has permitted above under sections 3 or 4, a~~An offender ~~shallwill~~ not have access to or possess a telecommunication device ~~while on Department of Corrections' property or in~~ any State vehicle.
 6. The Offender shall submit an Intent to Hire Form to the facility regarding the cellular telephone and/or computer, to include:
 - A. Computer:
 - (1) Location
 - (2) Location when not in use
 - (3) Make Model Serial #
 - (4) Passcode
 - (5) I.P. Address
 - B. Cellular Phone/Telecommunication device:
 - (1) Account holder
 - (2) Make _____ Model _____ Color _____
 - (3) Phone number
 - (4) Passcode
 - (5) Location when not in use
 - C. The Offender is responsible for updating the Intent to Hire Form with any changes.

143.03 APPLICABILITY

1. This Administrative Regulation requires an Operational Procedure for each institution and facility.
2. This Administrative Regulation requires an audit by the MIS-IT Division of all computer networks to which offenders have access at least once per year.

W. A. "Bill" Gittere, Acting Director

Date