SUMMARY of REVISION/REVIEW

APPROVED:

Scott R. Frakes, Director
Nebraska Department of Correctional Services
PURPOSE

This Policy provides guidance on acquisition and disposition, appropriate usage, and inventory procedures as they relate to computer equipment and software within the Nebraska Department of Correctional Services (NDCS). This Policy also provides guidance on the use of State telephones and information systems for inmate data usage. This policy applies to all NDCS staff, institutions/programs under NDCS jurisdiction and individuals under contract with NDCS.

GENERAL

NDCS Information Systems is responsible for the management of all NDCS acquired computer equipment, Kronos readers and software. All staff must adhere to all aspects of this Policy, for effective and efficient management of NDCS computer equipment, Kronos readers and software. Each institution/program shall adopt procedures consistent with this Policy. Wardens/program administrators are responsible for the gathering, accuracy, review, and verification of data entered into computerized information systems, as well as defining the content of reports generated from the data. Information Systems (IS) is responsible for the management of the data once it has been entered, the retrieval process, the safeguarding of the data to allow access only to individuals authorized by the wardens/program administrators, and the development and maintenance of applications using the data to produce reports at the request of wardens/program administrators or their designee. Information Systems and wardens/program administrators will work in partnership to develop new applications or new databases to meet changes in inmate data management requirements.

PROCEDURE

I. ACQUISITION AND DISPOSITION OF COMPUTING RESOURCES

A. Acquisition Procedure

1. Hardware and Software or Services

   a. Requesting Manager Responsibilities

   To request computer equipment, Kronos readers, software, or network devices (switches, routers, wireless access points) the requesting manager will submit an Information Technology Needs Assessment Form, with the Warden or Program Administrator’s endorsement to Information Systems for processing. Kronos badge reader requests must be initiated by facility HR contacts through the Human Talent Director. The IT Needs Assessment Form must include:

1) Warden or program administrator signature indicating approval of the request.

2) Business Manager signature

3) The computer user’s name and phone number.

4) The requester’s name and phone number.
5) Where the equipment will be located (facility, building, & room). For software only requests, include the IS Tag # of the PC the software is to be loaded on.

6) Justification/business case to support the request.

7) Business Unit billing information.

b. Information Systems Responsibility

Upon receipt of a request with the above information, Information Systems staff will evaluate the request. If the request is disapproved, a letter will be sent to the affected warden/program administrator explaining the reason(s) for the disapproval. If the request is approved, Information Systems staff will prepare a Material Request for Purchase (Form 263) and all other necessary documentation in accordance with Policy 113.06, Procurement. Information Systems staff will ensure the compatibility of all computer equipment and software prior to its purchase. Information Systems, through NDCS Purchasing, will order all computer equipment, software, maintenance services, computer-related training services, etc. Where possible, “loaner equipment” will be provided until the equipment is received. When the loaner equipment is new equipment comparable to what is ordered, it will remain in place and the ordered equipment will re-supply the loaner pool. Loaner equipment is equipment on-hand that is not a part of the Temporary Use Equipment as defined in section I.E.1.

2. Personal Equipment

No government data is allowed to be stored on personally owned computer equipment (including portable storage media) and, under no circumstance, is personally owned computer equipment, or software, permitted to be used in any NDCS facility.

3. Special Needs

Special needs requiring reasonable accommodation, i.e. visual impairment, physical disability, etc., are evaluated on a case-by-case basis by the Agency ADA Coordinator. Should special computer equipment or software be required, the supervisor and the Warden/Program Administrator will address the needs with the assistance of Information Systems.

4. Expendable Items

Computer printer paper, ink cartridges, toner cartridges, mouse pads, printer ribbons, CD blanks, diskettes, mice, keyboards, and USB storage devices are considered expendable items and will be purchased by the computer user through normal purchasing procedures according to Policy 113.06, Procurement. Due to the variety of connections and the need to install software drivers, other peripheral components are not considered expendable items. These items will be requested through Information Systems as outlined in Procedure I.A. above.
B. Installation of technology resources

1. Network installation
   a. General Information

   Installation of all data, voice, and digital camera cabling will be performed by staff or contractors certified in low voltage cabling installation. Network cabling will be approved by the Information Technology Manager.

   b. Requesting Manager Responsibilities

   To request network cabling, the requesting manager will submit an IT Needs Assessment to their Warden or Program Administrator or designee, program head or designated representative for endorsement. All endorsed requests must be forwarded to Information Systems for processing. The IT Needs Assessment Form must include:

   1) Warden/ Program Administrator or designee signature indicating approval of the request.
   2) Business Manager signature.
   3) The requester’s name and phone number.
   4) Where the cabling will be located (facility, building, & room number), along with a studies drawing or blueprint, reviewed and initialed by facility maintenance manager, indicating location of any network drops. (Contact Facility Maintenance Manager or NDCS Engineering for studies drawing or blueprint, if needed.)
   5) Justification/business case to support the request.
   6) Business Unit billing information.

   c. Information Systems Responsibility

   Upon receipt of an IT Needs Assessment with the above information, Information Systems staff will evaluate the request. If the request is disapproved, a letter will be sent to the affected institution warden or program administrator or designee explaining the reason(s) for the disapproval. If the request is approved, Information Systems staff will prepare either a Material Request for Purchase (Form 263) or a Nebraska Information System (NIS) Requisition document and all necessary documentation in accordance with Policy 113.06, Procurement.

2. Equipment Installation and maintenance
   a. Information Systems is responsible for the installation of all computer equipment, network devices and software. Information Systems staff
and qualified contractors working for Information Systems are the only persons authorized to configure and install computer software and networking devices for NDCS.

b. Computer enclosures may not be modified or opened. Contact the NDCS Information Systems Help Desk with your request. A qualified Information Systems technician will perform all maintenance and/or changes.

c. Additions or modifications to equipment or software

It is important that NDCS computers have a standard configuration. Unauthorized additions or modifications to equipment may result in a hardware or software malfunction. For this reason, no additions or modifications (e.g. sound cards, CD-ROM drives, extra printers, operational settings, etc.) will be made to NDCS computer equipment or software unless done by qualified IS staff or contractor staff approved by the Information Systems Manager. The Information Systems Help Desk, (402) 479-5865, should be contacted if a situation exists that requires an addition or modification of equipment or software. Information Systems will evaluate the request, make a determination, and promptly notify the requesting party.

3. Software installation, licensing and maintenance

In addition to network security, there are certain procedures that protect technology users, secure information, protect equipment, and ensure that warranties and copyright violations do not occur. All NDCS staff should adhere to the following:

a. Information Systems will purchase and install all software used in the NDCS environment. The software will only be installed on the NDCS computer for which it is licensed. All original software and documentation, except for user manuals, will be retained by NDCS Information Systems to safeguard against damage, loss, and unauthorized use. Information Systems will maintain records identifying software authorized for each computer. The records will contain the licensing and legal authority to use information.

b. All software must be properly licensed, registered, and installed as determined by Information Systems. Unauthorized or unlicensed software will be removed by Information Systems and reported to the area supervisor, Program Head, or Warden as deemed appropriate by the Information Systems Manager.

c. Information Systems will maintain a copy of all software licenses purchased by NDCS.

d. Software is copyrighted. It is illegal to make or distribute copies of copyrighted material without authorization. Software may not be installed on unauthorized or personal equipment. No software will be taken from the workplace for use at another location or for personal use.
e. Personal software will not be allowed on NDCS computers.

C. Movement of equipment and software

Non-IS NDCS staff are authorized to move, and reconnect computers with written approval. NDCS staff may obtain written approval by notifying the IS Help Desk of computer tag #, previous location, and new location. The Help Desk will provide email authorization for the move. Staff are only authorized to move systems and peripherals “whole” (i.e. all printers, monitors, and other equipment move together). IS staff is available, upon request, to assist with reconnecting equipment following moves.

D. Disposal of equipment and software

1. Hardware

Information Systems will determine if a computer is obsolete, no longer needed, or non-repairable. Equipment to be disposed of will have all software and data in the computer’s internal storage removed or destroyed. Disposal will be accomplished by a joint effort of NDCS Information Systems and NDCS Purchasing following the guidelines published by DAS Materiel. Disposal will be per DAS requirements.

2. Software

When software is no longer needed, Information Systems will erase it from the computer’s hard drive and dispose of all copies according to protocol. Software licenses, which can be reused, will be kept to meet future needs. Non-usable software will be destroyed in a manner specified by DAS Materiel.

E. Temporary Use Computing equipment

1. General

Information Systems maintains a limited number of laptops, projectors, USB storage devices, laptop speakers, web cameras, and digital cameras that may be checked out for short term use. This equipment can be reserved and checked out/in by contacting the IS Help Desk or IS Administrative Assistant. All equipment checked out must be individually signed for by the person who will be responsible for the equipment until it has been checked back in with Information Systems. A return date must be identified at the time the equipment is checked out. This equipment is available for staff attending conferences, attending training, traveling, and giving presentations. It is the responsibility of the person who checked out the equipment to ensure that all cables and accessories are returned with the appropriate equipment. If you have an ongoing need for any of this equipment, please fill out and submit an IT Needs Assessment Form. All cables are color coded to assist with placing them in the appropriate equipment bag. Cables with red tape go in the projector bag, cables with green tape go in the laptop bag, and cables with yellow tape go in with the speaker systems bag.

2. Central Office Conference Room Equipment
A mobile cart with a laptop and a projector is located in the four largest conference rooms in Central Office. The equipment is secured to the cart and is primarily for use in that conference room. Use of a cart at another location within Central office requires coordination with the NDCS Help Desk a minimum of two work days prior. Only Information System staff is authorized to remove equipment from the cart.

F. Special use Computing equipment

Fire, Life, Safety, Security, Environmental Control systems

Building automation, fire control, environmental control and security systems using the data network for connectivity, control, presentation and recording will be addressed individually, based on the particular need. These systems will usually be maintained by vendors under contract with NDCS. Where necessary, facility maintenance staff and engineering may be supporting some of these systems. Information Systems support requirements for these systems will be evaluated on a case-by-case basis by the Information Systems Manager in conjunction with the affected facility staff to ensure the most appropriate means of maintenance of the computer equipment and software which meets the needs of the system and the facility.

II. USE OF COMPUTING RESOURCES

A. Help Desk Resources

1. Assignment of User ID and Password.

All new FTE employees of NDCS are assigned NDCS Network access (Q and P drive access), and appropriate NICaMS system access upon entry into pre-service training. Usernames and passwords are provided to each employee during pre-service. Authorization is granted and documented through provision of new employee listing by HR.

Supervisors are responsible for requesting IDs and passwords for non FTE staff (contractors, etc.) and for requesting access to computing resources beyond basic network and NICaMS access. Assistance in completing these forms or information concerning who the appropriate IT Coordinator/Approver is can be obtained from the NDCS Help Desk at 402-479-5658. Access request types and processes include;

a. Access to CTS and CIT systems (mainframe access) - To obtain an ID and password, the supervisor will complete Attachment B (CICS1 ID Request/Authorization Form) and forward it to the appropriate facility IT Coordinator. The IT Coordinator will review the forms for completeness and accuracy before forwarding them to the NDCS Information Systems Help Desk. CIT access other than inquiry requires Accounting’s approval.

b. Access to CIPS (Corrections Inmate Payroll System). Attachment C is used to request access to CIPS and requires the additional approval of Accounting.
c. Access to other network resources, including Email, are submitted electronically through use of the Network Form. The Network Form is a paperless process. Signatures are not required. Paper forms and scanned forms are not accepted. Instructions and electronic documents are found at Q:\Computer Help\Computer Forms\Network Form Help. Forms may be initiated by supervisors or employees, but final submission to the Help Desk must be from a facility/program designated approver.

d. Access to additional NICaMS modules are provided following submission of an email request from a designated facility/program approver.

2. Termination of User ID and Password

When an employee leaves NDCS, it is required that the employee access to NDCS computing resources is blocked immediately or on their termination date.

a. During normal business hours, Human Resources will distribute current listings of employee’s separating from employment with NDCS. Information Systems (and any other organizational unit responsible for administering access control) will promptly eliminate all account access to employees identified (if not already removed). Absent a supervisor request for retention (through submission of a request to the help desk), network and email files will be deleted after 14 days.

b. After normal business hours, if an employee is terminated and the situation requires immediate removal of system access, the supervisor will notify the NDCS On-Call Information Systems Technician and Help Desk, in accordance with Policy 112.01, Clearance Process for Terminations, Resignations, Transfers, Promotions, and Demotions, Attachment B, Employee Clearance List. Notification must be made immediately via email, or by phone with a follow up by email, to ensure network, email, and other access is blocked.

c. When an employee transfers supervisors must promptly complete and submit to the NDCS Help Desk appropriate access request forms to remove, add, or adjust access to computing resources. Forms must be completed by both the former and current supervisor to assure only appropriate access is maintained.

3. Computing support and problem resolution

All new requests for computer assistance must start with the NDCS Help Desk

a. Contacting the Help Desk:

Email the help desk at dcs.help@nebraska.gov or call 402-479-5865. Please leave a voice mail if the phone is not answered or is busy. Night and weekend support is available on an emergency basis, but most support calls can and should be reported to the contacts above for resolution the next business day. Critical after-hours system outages (for example loss of network connectivity for an entire facility) should be
reported to the OCIO operations center at 402-471-4636. The OCIO Operations Center is staffed at all times, and will resolve problems or escalate them to NDCS on-call IT staff for immediate attention as required.

b. Information required includes:

1) Problem description
2) Your full name
3) Work location
4) Return phone number
5) Tag number of your computer (Example: IS1111)

c. All requests will be issued a work order number. Any issues not resolved at the help desk level will be given a priority rating and be escalated to other NDCS staff to complete.

d. Requests for Kronos repair must be generated by facility HR staff. If a potential problem is observed, the facility HR staff will contact the NDCS HR Director or designee. The HR Director or designee will determine if the problem should be escalated to the NDCS Help Desk.

B. Computing Security

The primary objective of computer security is to protect and assure confidentiality, integrity and availability of automated information systems and the data they contain. For this reason, it is important that all computer users adhere to the following procedures while using computers in the Department.

1. ID and Password Security

a. All computer passwords are confidential and will be assigned only to individuals authorized access. Passwords will be assigned an expiration period not to exceed 90 days. Shorter duration passwords will be used to safeguard network access and data access when tighter security is needed.

b. At no time will ID’s or passwords be shared or written down for others to see.

c. The following are the minimum password requirements for State of Nebraska passwords:

- Must contain a minimum of eight characters.
- Must contain at least three of the following four characteristics:
  - At least one uppercase character
  - At least one lowercase character
  - At least one numeric character
• At least one symbol
• Cannot repeat any of the passwords used during the previous 365 days.

Use care when creating a password, as the best passwords do not spell anything. The system will notify you if you do not meet this requirement and prompt you to select a new password that meets this strength standard. The Nebraska Information Technology Commission in conjunction with the Office of the Chief Information Officer has established a standard for passwords that meets the requirements of Neb. Rev. Stat. §86-516(6). This standard incorporates the characteristics identified above. The entire password standard is at http://nitc.ne.gov/standards/8-301.html

d. Do not post passwords. Do not maintain any listing of passwords near the computer, including “Post-it” notes, bulletin boards, posted on monitor or keyboards.

2. Data Security

NDCS employees are expected to save their data to their personal network storage (M) or work area shared (P) drive. Data stored on the local hard drive (C) is not backed up and may be lost in the event of a hard drive failure on the PC. Network drives (like M and P) are backed up nightly.

3. Data Privacy and Public Records

a. The (P) drive is available for sharing computer files within your program area or facility. Users shall not create shared folders on individual computers or any other location.

b. Information of a privileged nature, e.g. personnel evaluations/memos, should be stored on personal network storage (M drive).

c. All computer files, including those stored on personal network storage (i.e. M drives) are the property of NDCS and the State of Nebraska and are subject to being retrieved and viewed by authorized personnel at any time for any reason connected with official agency business. This information is generally retrievable from the system even after the file has been deleted.

d. Additionally, many NDCS computer files and e-mail messages are public records under the Public Records Act and are subject to being produced for public inspection upon receipt of a proper request unless there is some other legal basis to withhold the record e.g. attorney/client privilege, Mental Health record information, statutory confidentiality mandates and other specific exceptions allowing certain information to be withheld from public inspection.

e. Staff shall ensure when sharing data with individuals outside the agency that the information is accessible to the public as determined by Policy
4. Physical Security
   
a. All communications rooms and equipment cabinets will remain locked at all times. NDCS Information Systems, facility maintenance, and telephone repair personnel are pre-approved for access to these rooms; others requiring access must coordinate their request with the NDCS Information Systems Manager. Equipment that is not relevant to data or voice communications will not be stored in the communications rooms. All institutions are required to provide access to all communications rooms in their facility via a set of keys, which may be checked out to Information Systems Staff, or via an escort with a set of keys when Information Systems Staff require access to the communication rooms.

   b. Staff computers connected to the network or the state mainframe will not be left unattended and logged onto the NDCS network or the mainframe.

   c. Inmates will not be allowed to use staff computers or log onto the NDCS staff network. Inmates are only allowed to use computers designated for inmate use and labeled as such (see Policy 104.07, Inmate Computer Usage).

C. Acceptable Use

1. Staff shall operate within the limits of authority given in the normal course of duty when accessing any computer documents, files, data, or electronic mail.

2. The Nebraska Information Technology Commission (NITC) has established an Acceptable Use policy for the State of Nebraska State Data Communications Network. All NDCS staff and individuals under contract with the Department are required to comply with this policy. The policy is intended to provide minimum standards for acceptable use. All NDCS staff and individuals under contract are expected to make themselves familiar with the policy. NITC 7-101 Acceptable Use Policy may be reviewed at http://nitc.ne.gov/standards/7-101.html. Failure to abide by this policy can result in disciplinary action.

3. The Office of the CIO, Network Services has established the State Long Distance Policy governing the use of the State telephone network. All NDCS staff and individuals under contract with the Department are required to comply with this policy. This policy governs the provisions Neb. Rev. Stat. §81-1120.27 which states: “The facilities of the State’s telecommunications are provided for the conduct of state business. In addition, the state’s telecommunications network may be used by employees and officials for local and long distance calls to children at home, teachers, doctors, day care centers, baby sitters, to family members to inform them of unexpected schedule changes or for other essential personal business. The use of the State’s telecommunications systems for essential personal business shall be kept to a maximum of 10 minutes and shall not interfere with the conduct of state business. Essential personal long distance calls made on the State telecommunication equipment shall be either collect, charged to a third party, non-state number, or charged to a personal credit card”.

002.01, Access to Public Information. Public data is available on the Corrections website at http://www.corrections.nebraska.gov/

5. State of Nebraska (State) agencies issue cell phones/smart phones (device) to employees as needed. State employees must follow the procedures outlined below for NDCS employees regarding the use of state-issued devices.

NDCS issues cell phones/smart phones (device) to certain employees (‘individual’) as needed to complete job duties. NDCS issues cell phones/smart phones to certain post assignments (‘shared’). Facility Procedures will provide direction on maintaining accountability of ‘shared’ devices.

a. No ‘individual’ state-issued devices may be brought into any of the ten NDCS correctional institutions without prior written approval. A Cellular Device Institutional Request (Attachment E) will be used to request approval.

If approved, human resources will issue an institutional use card (card), which will include team member photo, name, title, phone number, brand and model of the phone. To be valid, the information on the card must be accurate. Approval is granted based on the position held; when a team member changes positions, a new request must be submitted.

b. Prior to proceeding past the first institutional check point, the card and authorized device will be presented for verification. The card will be retained at the access point, providing inventory and tracking control.

c. Upon exiting the institution, the device will be presented for verification, and the card returned to the individual.

d. Institutional use cards will be obtained for ‘shared’ devices in accordance with the facility’s Operational Memorandum.

State-issued devices may include camera or video functionality. Individuals issued such a device are required to abide by all departmental and institutional restrictions regarding photography in NDCS Institutions and facilities. The taking of photos/video must be approved, in advance, by the warden or communications office.

6. Contractors working within one of the ten NDCS institutions may need cellular devices to complete work. These devices must be approved, in advance, using the Cellular Device Institutional Use Request (Attachment E).

7. Connecting personal devices to State computing resources presents a variety of security and administrative concerns. Employees are not authorized to connect personal smart phones, or similar devices, to the State computing resources, including to State email accounts. Any connection of personal devices must be pre-authorized in accordance with NITC Standard 5-204, requiring approval by the State of Nebraska Information Security Officer and by the Director of NDCS.
a. Personal cellular devices are not allowed into NDCS correctional institutions. These devices may be stored in a designated area as defined by the facility procedure. Written exceptions may be granted by the Warden/designee on a one-time, case-by-case basis. Exceptions will be limited to those situations where there is a clearly demonstrated need for wireless phone access that cannot be addressed by any other means. The method for requesting an exception shall be outlined in the institution’s procedures.

8. Use of state equipment other than as permitted by law, accessing computer data without authority, or causing or allowing someone else to do so may result in discipline or other penalties as provided by Nebraska Statutes and/or applicable NDCS policies and procedures.

9. Additional guidance regarding acceptable use is provided in Policy 112.31, Code of Ethics and Conduct.

10. If a NDCS employee learns of a possible inappropriate use of NDCS computer equipment and/or software, it is his/her responsibility to immediately notify their supervisor. It is the supervisor’s responsibility to notify the Information Systems Manager of all such reports.

11. If, in the judgment of the NDCS Director, it is believed that unauthorized or criminal activity has taken place the Director may, at his or her direction, notify the proper authorities for investigation and possible prosecution.

D. Computer Related Training

1. All requests for computer-related training will be routed to the Information Systems Manager for approval in accordance with Policy 113.06, Procurement. This does not include tuition assistance training requests.

2. The computer classroom for NDCS is located at the Staff Training Academy. There are 20 student computers and one instructor computer connected to a projector. The computers are set up with access to Kronos, NICaMS, Microsoft Office Suite (Access, Excel, PowerPoint, and Word), Payroll and Financial Center (PFC), Telestaff, and Passport (mainframe). These computers are set up to work with Student IDs and DO NOT have Internet access. To reserve the computer classroom, please call the NDCS Staff Training Academy at (402) 471-1781. Advance notice of one week is needed to set up access to Internet websites or for other access not mentioned above. Please indicate any special access requirements when making a reservation.

E. Computer Related Investigations

Supervisors suspecting misuse or inappropriate use of computer-technology may submit a request to the Information Systems Manager for collection of computer records relating to the potential misuse. The Information Systems Manager will assign the appropriate Information Systems staff based on the nature of the suspected misuse or inappropriate use. If at any time during the investigation the Information Systems staff suspect a felony has been committed, they will immediately stop their investigation, contact the NDCS Investigators and the Information Systems Manager, and secure the equipment until it
can be picked up by a NDCS Investigator or State Patrol. A complete, detailed Incident Report will be written by the staff person finding potential felony activity. The Information Systems Manager will ensure that the NDCS Investigators, State Patrol (if applicable), and appropriate senior staff are immediately made aware of the findings and nature of the potential felony. All non-felony findings will be reported to the requesting supervisor, the Information Systems Manager, and appropriate senior staff.

III. INVENTORY OF COMPUTING RESOURCES

Information Systems in conjunction with each facility is responsible for the annual physical inventory of all computers and computer-related equipment within NDCS. The Information Systems Manager will ensure that all PFC barcoded equipment installed or moved is properly reported to the NDCS Inventory Coordinator for input into the Department of Administrative Services (DAS) statewide inventory system in accordance with Policy 113.04, Fixed Asset Inventory. Information Systems staff will complete the annual physical inventory and report all corrections in compliance with Policy 113.04.

A. PFC Tracked Assets

Generally, all computer towers, laptops, notebook computers, and tablet computers purchased are required to be listed in the Fixed Asset Inventory regardless of their cost. These systems will have a red and white barcode label attached to them. The barcode number will be assigned by the NDCS Inventory Coordinator. The NDCS Inventory Coordinator may identify additional equipment not meeting the purchase cost criteria for placement in the statewide inventory.

B. IS Tracked Assets

Information Systems will apply a separate barcode label to all computer equipment. These labels will have a solid background color and should not be confused with the red and white barcode labels used to identify assets in the PFC inventory. An IS inventory number will be on the tag when it is affixed. This number will be used for identification purposes when reporting a problem to the NDCS Help Desk.

C. Loaner Equipment

In addition to being tagged appropriately as determined in III A. and B. above, all equipment provided to a computer user as a “loaner” will also be tagged as “NDCS IS LOANER” and subject to the conditions of this Policy.

IV. INFORMATION MANAGEMENT AND INFORMATION SYSTEMS

A. Information-Gathering Criteria

The Research Department provides statistical and fiscal information of use to the administrators when making management decisions. Using NDCS goals and objectives as a guide, each warden/program head or their designee should identify their information needs to the Research Department. This includes specific criteria for evaluating overall institution performance and shall include specific descriptive terms used to classify inmates or to separate them by typologies. Consequently, the warden/program head will establish policies and procedures governing the collecting, recording, organizing, processing, and reporting of data developed for computerized information purposes.
B. Retrieval and Review

Wardens/program heads, Research, and IS will work together to maintain an organized system of information retrieval and review which is thorough, uniform, precise, and satisfies the requirements for inmate data keeping, research, and the decision-making process. The Research Department informs, and provides reports to the Director concerning Research and Management Information Systems data.

C. Review of System

Wardens/program heads or their designee will review their reporting requirements and research programs annually for applicability and desired enhancements. Additionally, the warden/program head or designee shall also review the computerized information systems’ policies with regard to the relevance and practicality of the information-gathering system and prepare a written evaluation; this report should be submitted in December. IS, Research, and wardens/program heads will work in partnership to make necessary changes or enhancements to the extent that technology and funding will allow.

D. Network Shared Drive Data Access

All Wardens and Program Administrators will designate an individual as the “Data Owner” of all data on their shared network drive. This person will be responsible for identifying to IS who is authorized access to the data in each folder and subfolder located on the facility/program area shared drive along with the degree of access (read only, read/modify/write, full access) for each person requesting access. IS will work with each facility/program area to refine the processes and establish the baseline environment for their shared drive.

E. Security and Verification

Data entered into computerized information systems shall be verified prior to entry. The accuracy of the data entered is the responsibility of the applicable institution/program head. The security of information shall at all times be maintained in accordance with Procedure I.A.5 of Policy 104.01, Inmate Records Management and Section II. B. of this Policy. Only designated individuals will have access to the information.

V. SHARING OF INFORMATION

Inmate data collected for computerized information systems may be exchanged on a Departmental basis. NDCS may collaborate with other criminal justice and service agencies in the information gathering, exchange, and standardization process. Inmate health data will comply with all Federal and State regulations.

VI. MASTER INDEX AND DAILY REPORTS

A. There shall be a single master index identifying all inmates assigned to the institution.

B. Each institution shall maintain a daily report of inmate population movement.

VII. PROGRAM INFORMATION
Institutional programs shall be analyzed and evaluated every year to determine their contribution to the institution’s mission.

REFERENCE

I. REGULATIONS AND POLICIES

Policy 104.04, Requests for Information and Public Records
Policy 104.07, Inmate Computer Use
Policy 112.01, Clearance Process for Terminations, Resignations, Transfers, Promotions and Demotions
Policy 112.31, Code of Ethics and Conduct
Policy 113.04, Physical Property Inventory
Policy 113.06, Procurement
Policy 113.08, Equipment Property Acquisition

Nebraska Department of Correctional Services Employee Handbook
State Data Communications Network Acceptable Use Policy
State of Nebraska Long Distance Policy
NITC Standard 5-204 Linking a Personal Portable Computing Device to the State Email System
NITC Standard 7-101 Acceptable Use Policy
NITC Standard 8-301 Password Standard

II. ATTACHMENTS

A. Information Technology Needs Assessment Form
B. CICS1 ID Request/Authorization Form for CTS/CIT Access
C. Network Authorization Request Form
D. CIPS Authorization Form
E. State Issued Cellular Device Institutional Use Request

III. AMERICAN CORRECTIONAL ASSOCIATION (ACA) STANDARDS

A. Standards for Adult Correctional Institutions (ACI) (4th edition): 4-4100; 4-4101; 4-4102; 4-4103; 4-4104; 4-4106
B. Performance Based Standards for Adult Community Residential Services (ACRS) (fourth edition): 4-ACRS-7D-05; 4-ACRS-7D-06
C. Standards for Administration of Correctional Agencies (CO) (2nd edition) 2-CO-1F-04