CD-044000 Information Technology Management	Issued: 08/20/01 Effective: 8/20/01	Reviewed: 5/28/19 Revised: 05/28/19
Alisha Tafoya Lucero, Cabinet Secretary		***Original Signed and Kept on File***

AUTHORITY:

A. NMSA 1978, Section 9-3-5(E), as amended.
B. NMSA 1978, Section 33-1-6, as amended.
C. Policy *CD-010100*.

REFERENCES:

A. ACA Standards 2-CO-1F-01, 2-CO-1F-02, 2-CO-1F-04, 2-CO-1F-06, and 2-CO-1F-08, *Standards for the Administration of Correctional Agencies*, 2nd Edition.
B. ACA Standards 4-4100, 4-4101, 4-4103 and 4-4106, *Standards for Adult Institutions*, 4th Edition.
C. ACA Standards 1-CTA-1D-01, *Standards for Correctional Training Academies*, 1st Edition.
D. ACA Standard 4-APPFS-3D-30 thru 4-APPFS-3D-32, and 4-APPFS-3D-36, *Standards for Adult Probation and Parole Field Services*, 4th Edition.
E. ACA Standards 2-CI-2C-1 and 2-CI-2C-2, *Standards for Correctional Industries*, 2nd Edition.
F. ICOTS Privacy Policy 3.0
G. ICOTS User Guide

PURPOSE:

Establish guidelines, policies and procedures which conform to Federal and State laws and regulations in regards to utilization of Information Technology within the New Mexico Corrections Department.

APPLICABILITY:

All NMCD employees and all employees who are bound by contract agreement with NMCD.

FORMS:

Policy/Procedure Acknowledgement form *(CD-044001.1)*
System Access Request form (*CD-044001.2)* – Located on NMCD intranet site.

ATTACHMENTS:

Offender Photo Name Board Sample Attachment (*CD-044006.A*)

DEFINITIONS:

A. *Access*: The ability to read, change or enter data using an information system.

B. *Bluetooth:* A standard for the short-range wireless interconnection of mobile phones, computers, and other electronic devices.

C. *Chief Information Officer (CIO)*: The Department's final authority on all Information Technology matters and the head of the Department's Information Technology Division.

D. *Cloud:* A network of remote servers hosted on the Internet and used to store, manage, and process data in place of local servers or personal computers.

E. *Contractor/Contract Staff*: An individual employed by a non-State entity under contractual authority granted by the State when the individual is working in a State-owned facility, or when the individual is using State-owned equipment.

F. *Contract Manager*: The individual assigned to supervise, direct and oversee the administration of a New Mexico Corrections Department (NMCD) contract.

G. *Download*: To receive a file transmitted over a network.

H. *DoIT* – State of New Mexico Department of Information Technology.

I. *Electronic Communications*: Includes, but is not limited to, electronic media and services such as computers, e-mail, telephones, digital-cellular phones, pagers, voice mail, fax machines, external electronic bulletin boards, chat rooms, news groups, wire services, on-line services, the Internet/Intranet, Web servers and browsers, terminal emulation (Telnet), file transfer activities (file transfer protocol), video conferencing and the World Wide Web.

J. *Employee*: An individual holding a position authorized by the State Personnel Office, a volunteer providing services to the State, or a docent providing services at a State museum facility.

K. *Encryption*: Encryption is the coding of data so that it cannot be understood by anyone without the equipment or code necessary to decipher the transmission.

L. *Equipment*: Computers, laptops, tablets, PDA's, mobile phones, monitors, keyboards, mice, routers, switches, hubs, software and any other information technology assets.

M. *Facility Administrator*: An individual assigned to extend Information Technology Division (ITD) support to users at a specific Corrections facility. This individual can access and modify the hardware or software configuration of a computer as needed and may be granted temporary system access as needed.

N. *ICOTS*: Interstate Compact Offender Tracking System

O. *ICOTS Administrator:* Individual assigned at NMCD that creates, deactivates and establishes roles for ICOTS users, and adds relevant case notes to State of NM cases.

P. *Information Classification*: State information is classified as public, proprietary or confidential. **Public information** is that which can be made freely available to the public. **Confidential information** is not available to the public either by law or

practice. **Proprietary information** is usually that which has a monetary value to its owner or originator, or which provides a competitive advantage to the business.

1) Public information can be provided to any State citizen upon request. Such requests may be subject to operational and financial constraints.
2) Confidential information is either proprietary State government property, private property or relates to the privacy of our customers and must be held in strictest confidence.
3) Confidential information should be stored in locked receptacles when not being used. Confidential information should not be stored in overhead receptacles or open bookshelves. This also applies to confidential information residing on computers, removable media (thumb drives, tapes, CD-ROMs, etc.) and hard-copy printouts.

Q. *ITD:* New Mexico Corrections Department Information Technology Division

R. *Information Technology/Information System*: Computer hardware, software, data bases, electronic message systems, communication equipment, computer networks and any information which is used by a State Agency to support programs or operations that is generated by, transmitted within, or stored on any electronic media.

S. *Internet*: A large network made up of a number of smaller interconnected networks.

T. *Local Area Network (LAN*): A communications network that serves users within a confined geographical area. It is made up of servers, workstations, a network operating system and a communications link.

U. *Malware:* Short for malicious software and is any type of software used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.

V. *PII:* Personally identifiable information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

W. *PDA: Portable Digital Assistant*: A mobile, hand-held device that can function both as a phone and as a computer, storing personal information, and may allow access to the internet.

X. *Password:* A word or code used as a security measure against unauthorized access to data.

Y. *Phishing:* An attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

Z. *Sexually Explicit Materials*: Images, documents or sounds that depict or imply exposed breasts, genitalia, oral sex, sexual penetration or sexual intercourse.

AA. *Shareware*: Software distributed on a trial basis through the Internet, online services, BBS's, mail order vendors and user groups. Shareware is software on the honor system. If you use it regularly, you're required to register and pay for it, for which you

will receive technical support and perhaps additional documentation or the next upgrade. Paid licenses are required for commercial distribution.

Spam: Irrelevant or inappropriate message sent on the internet, via email, to a large number of recipients in an attempt to gain sensitive information.

BB. *Upload:* To transmit a file over a network.

CC. *Wide Area Network (WAN*): A communications network that covers a wide geographic area, such as a State or country. A *LAN* is contained within a building or complex; a *MAN* (Metropolitan Area Network) generally covers a city or suburb.

DD. *Wireless Network (Wi-Fi):* A network that provides connectivity without the use of physical cables.

EE. *World Wide Web (www)*: The www. Prefix used on most Web addresses is actually the mnemonic name of the Web server used at the Web site.

POLICY:

A. All State or NMCD resources, including computers, laptops, tablets, servers, routers, storage devices, software, network, data, mobile phones, PDA's and telephone systems, whether leased or owned by the State, are to be used solely for the conduct of State business. However, personal computers may be used for personal correspondence as long as the use does not interfere with Corrections Department business and does not violate other provisions of this policy. Active determination of State business is the responsibility of the immediate supervisor.

Using agency goals and objectives as guidelines, agency staff shall identify information needs prior to the collection of data for the management information system.

1. Computers may not be used to develop programs for outside use.

2. Programs, spreadsheets or documents prepared using State resources or on State time are the sole properties of the State.

3. Work performed by contractors or using State resources is the sole property of the State. Exceptions must be specifically detailed in written contracts after the Department's legal review and CIO's or designee's review.

4. Personal software is not to be installed or run on State computer equipment without written approval from the CIO or designee.

5. Employees or contractors may not make copies of State-owned or leased software for outside use without permission of the agency CIO or designee, and then only in accordance with relevant licensing agreements.

6. Misuse of State or NMCD resources is prohibited and violators are subject to disciplinary action.

7. Employees have no right or expectation of privacy in documents, files or other information gathered or created while using State or NMCD resources. The State or NMCD reserves the right to read or inspect such information as needed.

8. All computer programs, software or projects developed, generated or created by State or Departmental employees while at work or on duty shall be the sole property of the State or the Department. Furthermore, all computer programs, software or projects developed, generated or created by State or Departmental employees for State or Department use or in connection with the employee's duties to the State or Department, shall remain the sole property of the State or Department, even if the programs, software or projects are developed, generated or created after normal work hours or away from the employee's work site.

B. The agency and institutions contribute to, have access to, and use an organized system of information storage, retrieval, and review. The information system is part of an overall decision-making and research capacity relating to both inmate and operational needs. **[2-CO-1F-02] [4-4100] [4-APPFS-3D-30]**

C. The New Mexico Corrections Department Training Academy has access to and uses an organized system, which may be automated, of information retention, storage, retrieval, and review. The information system has decision-making and research capacity relevant to both student and operational needs. **[1-CTA-1D-01]**

D. The Secretary of Corrections or designee ensures that field services data is collected, recorded, organized, processed and reported for information management purposes. **[4-APPFS-3D-31]**

E. All staff that has direct access to information in the information system is trained in and responsive to the system's security requirements. **[4-4101]**

F. There shall be a uniform collection, recording, organization, and processing of data developed for management purposes. **[2-CO-1F-01]**

G. The Secretary shall receive reports concerning research and management information from those responsible for the management information system. **[2-CO-1F-04]**

H. At a minimum, quarterly reports from those individuals in charge of the information system and research program are forwarded to the Secretary of Corrections or designee. **[4-APPFS-3D-32]**

I. The highest level of security shall be maintained in the New Mexico Corrections Department's efforts to preserve accurate and confidential records within its files, database programs and structures. This includes verification, access to data, and protection of the privacy of offenders and staff. **[2-CO-1F-06] [4-APPFS-3D-36]**

J. Security protocols and practices shall be established to protect the integrity of all correctional information and operating systems, including corrections industries. **[2- CI-2C-1]**

K. Correctional industries operations shall comply with the institution's requirements for data and system security. **[2-CI-2C-2]**

L. Each Department employee and contracted individuals with authorized sign-on privileges to the Department applications shall receive instructions on the proper accessing of said applications. It is the responsibility of staff managers that they obtain the ITD Information Systems Access form from the employee for before granting access.

M. There is a master index, readily available, identifying all inmates committed or assigned to the agency and/or each institution. **[2-CO-1F-08] [4-4103]**

N. The effectiveness of the information system as it relates to overall institutional management is evaluated in writing at least annually. **[4-4106]**

O. The intentional display of sexually explicit material or reproduction of sexually explicit sounds on any State information system is strictly prohibited, unless approved by a Division Director or above for the purpose of conducting official business.

P. State Internet facilities and computer equipment must not be used to violate the laws or regulations of the United States, any other nation, or the laws or regulations of any State or local jurisdiction in any material way.

Q. The NMCD will provide the appropriate communication services and equipment necessary to use the Internet for Department business.

R. The use of any State or Agency wireless networks or PDA as a mechanism to connect personal devices to the Internet, such as using a State-issued mobile phone as a wireless hot-spot for a personal device, is strictly prohibited.

S. All employees and contractors granted Internet access will be provided with a written copy of this policy and must sign the acknowledgement, which will be kept on file by the NMCD-IT.

CD-044001 Security	Issued: 08/20/01 Effective: 8/20/01	Reviewed: 5/28/19 Revised: 05/28/19
Alisha Tafoya Lucero, Cabinet Secretary		***Original Signed and Kept on File***

AUTHORITY:

Policy *CD-044000*

PROCEDURES: [2-CI-2C-1]

A. Computer Systems Access: [4-4101]

The highest level of security shall be maintained in the New Mexico Corrections Department's efforts to preserve accurate and confidential records within its files and database programs and structures. This includes verification, access to data, and protection of the privacy of offenders and staff. **[2-CO-1F-06] [4-APPFS-3D-36]**

Access authority will be protected by following these measures:

1. Each Department employee, including Corrections Industries **[2-CI-2C-2]** and contractors with authorized sign-on privileges to the Department applications shall receive instructions on how to access authorized applications. It is the responsibility of staff managers to obtain and complete the ITD Information Systems Access Request (SAR) form from the internal NMCD intranet site and submit it to NMCD-IT.

2. Unit managers (State or contractor) will fill out a Login ID and SAR form and submit it to the ITD for each computer user. Should an employee or contractor change jobs within the agency, a new form must be submitted and all previous privileges be removed within a reasonable period of time.

3. Records of ID authorization will be maintained electronically and stored for auditing.

4. Employees and contractors will be given access only to information and programs required for their assigned job duties. Contractors receiving IDs will be considered as having temporary permission and therefore the security processing form must indicate that they are temporary. The period of authorization should reflect the contractual agreement end date.

5. LAN Administrators will issue network IDs of between eight and 15 alphanumeric characters.

6. The ITD shall disable computer accounts used by contract personnel upon notification by agency personnel responsible for the contract that the contract is completed, terminated or notification that the formerly authorized user is no longer governed by the contract.

7. The ITD will be immediately notified by the employee's manager when an employee leaves the agency permanently, for a period exceeding 30 days, or in the event of being placed on administrative leave due to a pending investigation. The ITD will disable/delete that employee's computer accounts. The former employee's Supervisor will work with the system administrator to ensure that all necessary computer files are accessed and saved prior to deleting that employee's computer account.

8. The contractor will immediately notify ITD when an authorized user has left the contractor's employment. No other user may access or process under another contract user. Violation of policy is considered a breach of security and will be reviewed by the CIO or designee and Contract Representative.

9. The Information Technology Division (ITD) manager, NMCD Division Director, and/or Human Resources must notify the CIO or designee of employees to be involuntarily terminated and the time/date of the termination (preferably prior to the event) so as to allow discontinuation of that employee's computer access.

10. Termination procedures require that the Login ID & Systems Access Request be signed and dated to remove the access an employee had been given. Access to a given program will not pass on to another employee without having the proper forms submitted. When termination occurs, final paperwork will reside with the ITD Security Officer.

B. Password Controls:

Passwords must be controlled to prevent their disclosure to or discovery by unauthorized person(s). Managers should plan ahead and notify ITD of new hires or other personnel changes prior to the effective date of the employee needing system access.

1. Corrections Department's LAN Administrator will issue the default password to a new user. Upon initial sign-on to the network, the user will be required to change the password immediately.

2. Each individual user shall have his or her own unique password(s) that should never be shared with another person or supervisor.

3. If passwords must be written down because of security or operational requirements, they must be kept on your person.

4. Passwords will be of at least six characters in length. Users must use at least one numeric digit within the passwords, but not

in the first position. Passwords should not be words published in a Webster's standard dictionary, or be family names, pet names, birthdays, social security numbers, etc.

5. Passwords assigned to Department employees with authorized sign-on privileges to Department applications shall be changed at ninety (90) day intervals. ITD shall automatically schedule password changes.

6. Employees or contractors will be prompted by the sign-on process when a password change is required. Users will be responsible for changing their own password.

7. The user sign-on shall be disabled after three unsuccessful login attempts on systems supporting this function. To become reactivated, the employee or contractor must notify their supervisor so that they may contact the ITD User Help Desk to have the password activated.

8. Administrative passwords will be maintained by the ITD.

9. No password privileges shall be shared by another individual. This unauthorized use could make the employee or contractor liable for any actions that were invoked by the use of the ID and password.

10. Any employee suspecting unauthorized usage of his or her password privileges must follow established guidelines or have passwords re-issued. The employee is obligated to report suspensions to the Security Officer.

11. Any misuse of password usage by employee or contractor may result in disciplinary action or criminal prosecution under federal copyright laws.

12. Default operating system software screen saver program must be invoked to identify any unauthorized access occurring to the system and PC. It is the responsibility of the employee to make sure that they are properly logged out of any program and the PC at the end of the employee's work day.

13. The Local System Administrator or super user IDs must be assigned by the Security Officer, CIO or designee. These system accounts are maintained and secured with limited access by Active Directory security.

14. Common or group passwords will be used only in cases where the system or software does not support multiple users, or when testing software systems are in process.

C. Access Controls:

Physical and logical controls must ensure that users cannot access stored information unless they are authorized to do so.

1. File servers and other multi-user or sensitive systems should be kept in locked, limited access rooms. Computer lock keys must be sealed and locked in security cabinets.

2. Visitors or unauthorized personnel must be escorted in areas containing sensitive computer systems. When a visitor is required to access other highly sensitive areas, such computer/network areas, they will be required to show their badge and sign in on the Visitor's Log in the ITD area. Violations to this policy will not be tolerated. Visitors and unauthorized personnel in the secured areas may not open the area to any other unauthorized person; only ITD staff members may allow access to restricted areas.

3. Unmanaged system configurations are not allowed on NMCD computers or supported by ITD staff. Wireless cards (Air Cards) or Smartphone Hotspots are supported by ITD staff on Department issued laptops and/or mobile devices using a virtual private networking (VPN) solution.

4. USB data drives, flash drives, thumb drives, memory drives, wireless data access devices, MP3 devices, iPods, any other technology or storage devices are not allowed in any Prison Facility unless a written request is made to and authorized by the CIO or designee.

5. All personal devices that communicate wirelessly, including activity fitness trackers and smart watches, are prohibited from being brought into any Prison Facility, as these devices have the capability to communicate with other devices over a wireless transmission protocol such as Bluetooth, Wi-Fi and cellular.

6. Access to tape backups should be limited to those responsible for handling the tapes.

7. Non-employees are not allowed to use State computer equipment or software except as authorized by the Division manager (this includes employee's spouse or children),

8. Violations of access controls must be reported and recorded for review by the CIO or designee.

9. Managers and contractor supervisors are responsible for notifying the IT Security Officer or Human Resources office concerning persons no longer allowed access to the building.

10. Offenders in the custody or supervision of the Department will not be allowed access to any computer connected to the State of New Mexico network. Offenders may only use State owned computer equipment for authorized educational or vocational purposes.

D. Data Validity/Security:

Controls must ensure accurate data capture and data entry, including detection and correction of errors.

1. Managers are responsible for ensuring, through data entry personnel, that information entered into the computer systems is valid and accurate.
2. The same controls should be applied to data edits as required for original entry.

3. Error reports will be issued on a weekly basis to the appropriate data entry personnel for modifications.

4. All new personnel who are required to access confidential information will follow this process:

    a. *Security Awareness*: Procedures dictate that all NEW or returning employees should be provided the policies and procedures regarding their responsibilities to security awareness.. Information regarding security awareness will be included in the NMCD onboarding package for employees to review.

    b. *Manager/Supervisor*: The responsible manager will define the information, if any, that the employee will have access to and complete the necessary SAR form and submit to IT to get the security approval for the employee in a timely manner.

    c. *Security Permissions*: The IT Help Desk will review, create and test the security permissions before forwarding to the user. It is the responsibility of IT to make sure that the ID assigned to the personnel is USER READY. Copies of approved SAR forms will be kept on file.

    d. *Notification*: The IT Help Desk will notify the user that their ID has been established. It will also be forwarded to the Training Academy Coordinator to make sure that office is aware that there may be a need for training regarding the accessibility of a secured program.

5. Data shall not be shared with any outside entity without the review and prior approval of the appropriate Agency administrator. Further, all data entered into IT systems shall only be utilized for its intended purpose to conduct necessary Agency operations.

E. Audits:

1. Audits will be performed on computers periodically. Any irregularities will be documented and forwarded to the Division head and CIO or designee.

2. Measurements will be established to make sure that hardware and software enhancements are placed in the appropriate locations to ensure confidentiality.

3. The ITD's Information Systems Access policy shall be read, examined and acknowledged by signature from each Departmental staff member. These forms will be maintained by the ITD Security Officer in a secured area.

Form CD-044001.1
Revised 05/28/19

NEW MEXICO CORRECTIONS DEPARTMENT
Policy/Procedure Acknowledgement

*I,*_____*, ACKNOWLEDGE THAT I HAVE RECEIVED*
(PRINT NAME)

A copy of the Information Technology Management policy and associated procedures and that it is my responsibility to read and comply with it. I further acknowledge that I understand that violations of this policy/procedure may result in disciplinary action. I understand that if I have questions, or I do not understand any provisions of this policy/procedure, I will ask my supervisor for assistance.

_____ _____
Employee Signature Date

_____ _____
Witness Signature Date

Original = Employee File
Copy = Employee

CD-044002 Hardware	Issued: 08/20/01 Effective: 8/20/01	Reviewed: 5/28/19 Revised: 05/28/19
Alisha Tafoya Lucero, Cabinet Secretary		***Original Signed and Kept on File***

AUTHORITY:

Policy *CD-044000*

PROCEDURES:

A. Hardware Acquisitions:

1. All information Technology equipment to include but not limited to desktops, laptops, smart phones, mobile devices, tablets, kiosks, Digital Video Recorders (DVR's), IP cameras, etc. for the Department, custody, non-custody staff and inmate use, including facility inmate stores, must be approved by the CIO or designee.

2. To obtain purchase approval on hardware, new workstations and existing workstations must meet the minimum baseline workstation configuration. Corrections Department ITD standards are available for review in the IT Division. State standards may be viewed via the Internet.

3. New PC acquisitions must submit an ITD work order to have users and workstations added to the Corrections Department's network.

4. If equipment does not meet these standards, the equipment will not be able to run the standard core software suite. The software standards will identify products that the IT Division is committed to providing help desk service and promoting office-to-office compatibility of resources.

B. Moving Equipment:

1. Only authorized ITD personnel may move, transfer or relocate computer equipment and peripherals unless the Infrastructure manager has given permission to an on-site representative. This ensures that handling has been done properly and there is no needless damage to the equipment or injury to the employee.

2. Hardware movement should only be necessary when: network access has become breached; access is impossible due to a natural disaster; Departmental emergency movement or facility relocation. Movement in remote locations should be approved by ITD and electronically acknowledged as to who is the authorized Representative in the remote location. Authorization must be given prior to movement.

C. Virus Protection:

To ensure that a computer virus is not introduced into the Department's network or information system by a personal computer or a contractor personal computer, the users must follow these guidelines:

a. If the program or subject is coming from the Internet, it must first be placed on flash drive or compact disc/DVD and then an anti-virus program must be scanned on the flashdrive/compact disc/DVD. If the object is too big for flashdrive, DVDor compact disc, contact the LAN Administrator for assistance.

b. All flash drives and compact discs/DVD must be scanned by the anti-virus software that has been placed on the CPU whether done automatically or manually by the user. Users should be aware that when information is received or sent from a workstation on the LAN/WAN, if identified as a virus, a security report is emailed to the LAN Administrators for record.

c. New acquisitions for any Corrections Division MUST include the purchase of licenses for department standard anti-virus software.

d. Any contractor equipment that has been approved for connection to the Network must comply to the hardware specifications to ensure compatibility with the Corrections network and the appropriate virus software enabled.

e. Any existing machine must be updated with virus protection or be subject to REMOVAL from the Corrections Department's network.

CD-044003 Software	Issued: 08/20/01 Effective: 8/20/01	Reviewed: 5/28/19 Revised: 05/28/19
Alisha Tafoya Lucero, Cabinet Secretary		***Original Signed and Kept on File***

AUTHORITY:

Policy *CD-044000*

PROCEDURES:

A. Department users shall not duplicate any licensed software or related documentation for use either on Department premises or other designated work areas unless authorized by the CIO or designee.

B. Users are not authorized to give software to any individual or groups considered non-Departmental employees. Department users may use software on local and area networks or on multiple machines only in accordance with applicable license agreements.

C. Fundamental guidelines to the protection of Departmental computer equipment:

1. All PCs, standalone or attached to the network will use only the adopted Windows operating system unless authorized by the CIO or designee.

2. Information Technology Division staff supports only Microsoft Office Products for office automation, i.e., document and spreadsheet creation, email, presentation, etc.

3. No software will reside on any Department computer without a valid software license. Any software found on computers without valid licenses will be removed and the incident will be recorded and the employee(s) responsible will be subject to disciplinary action.

4. Software shall not to be downloaded through the Internet without the authorization of the Information Technology Division. Requests must be in writing and submitted to the CIO or designee.

5. To maintain the support and licensing requirements, ITD personnel or their representatives will be solely responsible for installing and removing authorized software on Department hardware. Prior to being installed on Department equipment, all software must be approved by the department CIO or designee.

6. Software not on the pre-approved list will be approved for acquisition on a case- by-case basis. Requests should be forwarded to the CIO or designee. A copy of the pre-approved list may be obtained by contacting the Workstation group.

7. Any software that is not compatible with the operating system will be removed.

8. Any personal software loaded on a Department computer will be recognized as State property and inventoried as such.

9. Any person loading software without written authorization shall be subject to disciplinary action.

10. Users and contractors are not permitted to bring software from home and load it into the Department and network computers.

11. If Department-purchased software permits home/work environment with only the need of a single license, the user must be given permission for such use by the CIO or designee. A record of the dual workstation license will be recorded in the proper database files.

12. The Department will abstain from purchasing or using shareware products. Only authorized ITD staff may install and configure shareware to work on computer environment. All compatible shareware software may be considered as an exemption, but should be approved by the immediate supervisor. If the supervisor feels that the software should be investigated and deemed as compatible, he/she should contact the ITD for the proper authorization.

13. There shall be a uniform collection, recording, organization, and processing of software data developed for management purposes. **[2-CO-1F-01]**

E. U.S. Copyright Act of 1997:

1. Illegal reproduction of software is subject to civil damages up to $100,000 per title infringed and criminal penalties including fines up to $250,000 per title infringed and imprisonment of up to five years.

2. Unauthorized duplication of software may subject users and/or the Department to both civil and criminal penalties under this act.

3. Users found distributing or storing of music or video media such as MP3's, MP4's, AVI's, WMA's and WMV's on state-owned equipment such as servers, workstations and file shares shall be subject to disciplinary action. The user could also face criminal charges, state or federal, due to infringing activity on state-owned servers and workstations.

4. Use of any Peer to Peer application (downloading of movies, music or other copyrighted material) by staff is prohibited on any state-owned computers.

F. Workstation Standards:

1. The ITD established the workstation standards to assist and aid the various departmental units when acquiring software in their area. A copy of these standards is available for review in the ITD.

A. The New Mexico Department of Information Technology issued the NMAC Rules which are the foundation for the ITD standards and procedures. All employees may view the DoIT Rules via the Internet.

G. Operations:

All locations are required to submit a Security-Software form to the ITD to receive permission to purchase or upgrade existing software that is not covered in the Personal Computer software workstation standards.

CD-044004 Electronic Mail	Issued: 08/20/01 Effective: 8/20/01	Reviewed: 5/28/19 Revised: 05/28/19
Alisha Tafoya Lucero, Cabinet Secretary		***Original Signed and Kept on File***

AUTHORITY:

Policy *CD-044000*

PROCEDURES:

A. Use of Electronic Mail:

The use of email within NMCD shall be used for business purposes only. Access to personal email accounts and/or external email providers, such as Yahoo!, Gmail, Dropbox, etc., from NM State-owned equipment and utilizing NM State network shall not be allowed without prior exception/approval from Executive Management and IT.

B. Monitoring of Electronic Mail:

Any messages sent or received via the email system may be monitored by said offices, with or without prior notification. Electronic mail provided by the NMCD is considered to be owned by the NMCD.

If, through electronic monitoring, the potential of misconduct or criminal activity has been discovered, the information contained in such electronic messages may be used to document such conduct and will be revealed to the appropriate authorities.

C. Electronic Mail Security:

Email accounts are to be used only by authorized participant accounts for authorized use only. Participants may designate other authorized personnel access to their scheduling and receiving queues of their electronic mail software program, but account owners are ultimately responsible for all activities under their account.

Impersonating another user or otherwise falsifying one's user name in electronic mail is strictly prohibited.

D. Record Keeping/Archiving Electronic Mail Messages:

Any message sent or received that is relevant to the course of business should be printed or stored in electronic form on ITD LAN/WAN servers and retained based on the NMCD retention requirements. Any excessive buildup of old and unread messages in the user's box should be cleaned out periodically according to the number of messages the user receives. DoIT as the owner of the Enterprise email system is responsible for

backing up all electronic forms and messages.

E. Appropriate Use of Mailing List or Discussion Groups:

Subscriptions to mailing lists, bulletin boards, chat groups, social media sites and commercial online services and other information services may be given for limited purposes if they are pertinent to the employee's job. Requests must be submitted for review and approval of the CIO or designee prior to access or use.

F. Electronic Mail Signatures:

If a message that originates from your account could be perceived as Corrections Department business or opinions, but it is not officially representing the Corrections Department, a disclaimer is to be included on your signature. The disclaimer is "**The opinions expressed here are my own and do not necessarily reflect those of the Corrections Department**".

G. Sending Attached Documents Via Electronic Mail:

It is permissible to transmit documents via electronic mail as attachments. However, transmitting copyrighted material, including software and applications programs, without consent of the copyright holder is strictly prohibited. Additionally, it is the responsibility of each employee to ensure that PII is redacted and not included in any email communication.

If the information exceeds the Information Systems/DoIT permissible allocation of 20 MB bytes of information, the user will need to contact the IT Division for assistance. If the document is being moved from one location to another location within the agency, contact the LAN Administrator to check on the creation of a folder environment instead of email. Make sure that the receiver does not also have file size limits for incoming messages or attachments. Documents that should be made available to numerous NMCD employees should be posted on the NMCD Intranet and the email should contain the necessary link.

If using the standard email software, compression is available and therefore the user may have to compress the information before attaching to the message.

H. Electronic Mail With Corrections Department Attorneys:

Correspondence to or from any Corrections Department Attorney on any legal matter is considered privileged and confidential. DO NOT send copies of the messages to anyone else. If you believe the message should be shared with someone else, ask the attorney(s) to forward the message to the appropriate individual.

I. Unsolicited Advertisement/Promotions:

It is illegal under United States federal law (US Code Title 47, Sec.227 (a) (2) (b)) to send unsolicited advertisements via email. Therefore, Corrections Department

employees should not receive any unsolicited advertisements or promotions, and if received, should notify the IT Security Officer.

J. Electronic Mail Harassment:

The Corrections Department will investigate any and all reports of attempted use of electronic mail for harassment. Such acts include, but are not limited to:

- Sending threatening, harassing or abusive messages;
- Sending sexually explicit graphics or text messages; and
- Sending hate mail.

If the results of the investigation reveal that such acts have been committed, disciplinary actions or termination may result.

K. Misuse of Electronic Mail:

Acts considered a misuse of electronic mail and subject to discipline or sanctions are:

- Engaging in illegal activities.
- Giving away information about other electronic mail users to allow other non-users to access or use account (without consent of user or agency).
- Accessing and/or using other accounts without their permission.
- The user may not send unsolicited bulk mail; email containing illegal material such as chain letters involving money or goods; email containing material protected by copyright, trademark or trade secrets; and email that is considered forbidden by the laws of applicable countries and States.

L. External Electronic Mail Agents:

Access to personal Electronic Mail Provider accounts (such as America Online, Hotmail,Gmail, Yahoo, etc.) is prohibited over State networks unless there is a valid business reason for such access. Any exceptions must have prior approval from the CIO or designee and recorded on the file.

M. Operations:

1. To report any misuse of electronic mail policies, contact the ITD Security Officer. Provide to the officer your name, location, the name of the individual violating the policy and a description of the violation.

2. Any individual receiving unsolicited offensive electronic mail, not received as part of official business, MUST CONTACT the ITD Security Officer. The receiver of the mail must NOT DELETE the message. The Security Officer will instruct the user on archiving and hard copying the message for further investigation. The Security Officer will submit an Incident Report to the CIO or designee, who will pass it on to the Office of Professional Standards to conduct an investigation.

3. Violators and others involved in the violation are subject to disciplinary action.

If any Corrections employee has questions regarding electronic mail, he or she should contact the IT Division or IT Security Officer.

N. Spam/Phishing/Malware

1. It is the responsibility of each NMCD employee to be vigilant in not responding to emails of unknown/untrusted origin, or opening potentially dangerous emails/email attachments that could expose the agency to the compromise of system security, the loss of critical data or the disruption of business operations.

2. NMCD IT and other NM State Agencies, such as DoIT, will never ask for your email credentials via an email. It is the responsibility of each NMCD employee to not provide email login credentials to any other individual.

3. Any email that is suspected to be an attempt to compromise system security or to obtain information to disrupt operations shall be brought to the attention of IT Help Desk or IT Security immediately.

CD-044005 Internet Usage	Issued: 08/20/01 Effective: 8/20/01	Reviewed: 5/28/19 Revised: 05/28/19
Alisha Tafoya Lucero, Cabinet Secretary		***Original Signed and Kept on File***

AUTHORITY:

Policy *CD-044000*

PROCEDURES:

A. Management and Administration:

1. Any employee or contractor who uses Corrections Department hardware or software to access the Internet does not have any expectation of privacy as to his or her Internet use.

2. Management may review Internet activity and analyze usage patterns to ensure Internet access is used exclusively for State business.

3. Employees and contractors should schedule equipment-intensive operations, such as large file transfers, video downloads, or mass emailings, for off-peak times.

B. Access is a Business Tool:

1. State employees and contractors must conduct themselves honestly and appropriately on the Internet and must respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others, as in any other business dealings.

2. All existing State of New Mexico policies apply to employee and contractor conduct on the Internet, particularly those that relate to intellectual property protection, privacy, misuse of State equipment, sexual harassment, hostile work environment, data security and confidentiality.

C. Maintenance of the State's Image and Posture:

1. Anything an employee or contractor communicates on the Internet can be interpreted as representing State government. Any person abusing or violating any of these guidelines is subject to disciplinary action.

2. Each employee or contractor using Internet facilities provided by the State shall identify him or herself honestly, accurately and completely (including State affiliation and function where requested) when participating in chats or newsgroups, social media sites or when setting up accounts to use outside computer systems.

3. Only those employees and contractors who are authorized by a State supervisor to speak to the media, to analysts or in public gatherings on behalf of the State may speak/write in the name of the State to any newsgroup or chat room. Other employees or contractors may participate in newsgroups, social media sites or chats when relevant to their duties, but they do so as individuals speaking only for themselves.

4. When a participant is identified as a representative of the State, an employee or contractor must comply with laws governing political speech.

5. The State retains the right to any material posted to any social media site, forum, newsgroup, chat or the World Wide Web by any employee or contractor in the course of his or her duties or employment.

6. Employees and contractors are reminded that social media sites, chats and newsgroups are public forums where it is inappropriate to reveal confidential information, client data, or any other information covered by existing State confidentiality policies, procedures or contract terms.

7. Employees and contractors releasing confidential information via social media sites, newsgroup or chat will be subject to sanctions and disciplinary actions associated with existing policies and procedures.

D. Internet Safety:

1. Access to the Internet can enable unauthorized external access to State data and networks if employees and contractors do not apply appropriate security discipline.

2. Computers with confidential data or mission critical applications may be prevented from connecting to the Internet in accordance with program and security requirements.

3. Agency managers shall hold users accountable for any breaches of security or confidentiality.

4. The State reserves the right to inspect any and all files stored on any State-owned computer.

5. Any file that is downloaded via the Internet must be scanned for viruses before it is run or accessed.

6. Computers that use wireless Internet access cards can be used by an attacker to compromise any network to which these computers are connected. Any State computer used for external dial-up , leased-line modem or wireless connections to any outside computer or network must be physically isolated from the State's network or protected through a virtual private network and firewall.

E. Sexually Explicit Materials:

1. Sexually explicit material may not be displayed, accessed, stored, distributed, edited or recorded using State network or computing equipment, unless approved by a Division Director or above for the purpose of conducting official business.

2. Employees or contractors who inadvertently connect to a site containing sexually explicit material must disconnect from that site immediately.

3. In offices where display or use of sexually explicit material falls within legitimate job responsibilities, a direct State supervisor may exempt affected employees or contractors from this policy. This exemption must be provided in writing and filed with the Information Technology Division.

F. Use of the Internet for Illegal Purposes:

1. Use of any State equipment for illegal activity is grounds for disciplinary action, up to and including dismissal.

2. Use of State Internet access to commit infractions, such as misuse of State assets or equipment, sexual harassment, unauthorized public speaking, misappropriation or theft of intellectual property is strictly prohibited.

3. Employees and contractors with Internet access must understand copyright, trademark, libel, slander and public speech control laws of all countries in which the State of New Mexico maintains a program presence to ensure that Internet use does not violate any laws which might be enforceable against the State.

4. The Corrections Department will cooperate with any legitimate law enforcement activity.

G. Ownership of Downloaded Material:

1. Any software or files downloaded via the Internet onto State computers becomes the property of the State.

2. Software may be downloaded from the Internet only after obtaining approval from the agency's CIO, designee, or equivalent.

3. Any downloaded files or software may be used only in ways that are consistent with their licenses or copyrights.

4. No employee or contractor may use State equipment to download or distribute pirated software or data.

H. Improper Usage of the Internet:

1. No employee or contractor may use State network access to deliberately propagate any malware, such as a virus, worm, Trojan horse, or trap-door program.

2. No employee or contractor may use State Internet access to intentionally disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of data.

3. Access to personal Internet Service Provider accounts, such as America Online, is prohibited over State networks without ITD approval.

I. Use of Internet News Services:

Employee or contractor use of news briefing services (e.g. RSS, weather and stock feeds) is acceptable, unless agency management determines such usage places unacceptable burdens on network equipment.

J. Off-Hours Browsing:

State supervisors of employees and contractors shall grant permission to use Internet access for non-business research or browsing during mealtime or other breaks, or outside of working hours, provided that all other Internet usage policies are adhered to and additional State money is not used for personal and non-business purposes.

K. Abuse of State Licenses:

Employees and contractors with Internet access are prohibited from uploading any software licensed to the State or data owned or licensed by the State without explicit authorization from the manager responsible for the software or data.

L. Secure Use:

1. Any employee or contractor who attempts to disable, defeat or circumvent any State security mechanism (firewall, proxy, Internet address screening program or other security system) will be subject to sanctions or disciplinary action, up to and including dismissal.

2. Any computer used as a Secure File Transfer Protocol (SFTP) server must be isolated from all servers that contain mission critical applications or confidential data. These SFTP client computers may not host any mission critical applications or confidential data.

3. The Chief Information Officer or designee may authorize qualified State or contract personnel to test firewalls or network security mechanisms operated by State agencies.

4. Because the potential exists for security testing to disrupt network operations, the host agency's cabinet secretary and the ITD manager (or their equivalents) must be notified in writing at least one week prior to testing.

M. Inmate Use:

1. Offenders in the custody or supervision of the Department are **not** permitted access to the Internet, nor are they permitted to obtain access to the Internet through third parties.
2. Inmates may be granted limited access to the Internet to complete educational requirements, or take tests such as the GED.

CD-044006 Information Systems and Research	Issued: 08/20/01 Effective: 8/20/01	Reviewed: 5/28/19 Revised: 05/28/19
Alisha Tafoya Lucero, Cabinet Secretary		***Original Signed and Kept on File***

AUTHORITY:

Policy *CD-044000*

PROCEDURES: **[4-4100]**

A. Criminal Management Information System (CMIS): [4-APPFS-3D-30]

CMIS is designed to capture data as the offender flows through the correctional system process from entering the jurisdiction of the department through final discharge.

1. CMIS shall be designed, developed, enhanced and maintained to meet the Departments' business requirements for managing offenders under NMCD jurisdiction.

2. CMIS will have various levels of built-in security. This security will restrict the users to areas of information pertaining to their job duties and restrict them from other areas of information in the system. Security access to the data will be granted via established business roles. Security will also be available at the screen and table level.

3. The integrity of the system data tables, structures, backup and recovery is provided by the Information Technology Division.

4. Data integrity and data dissemination is the responsibility of each division.

5. CMIS program enhancements are coordinated through a shared development within the National Consortium for Offender Management System (NCOMS). NCOMS is comprised of multiple State Corrections Departments. The NCOMS member states have signed agreements to standardize design, development and data. This provides for NCOMS members to maximize public funds and share data with governmental agencies and justice entities.

6. The Secretary shall receive reports concerning research and management information from those responsible for the management information system and research program. **[2-CO-1F-04]**

7. CMIS reports will be provided to the agency administrator. Reports will be generated daily, weekly and quarterly and provide the agency administrators

summaries of offender population to include: population trends, characteristics, movement and other demographic information. **[2-CO-1F-04]**

8. CMIS will provide a master index, readily available, identifying all inmates committed or assigned to the agency. **[2-CO-1F-08]**

9. The Secretary of Corrections or designee ensures that field services data collected, recorded, organized, processed, and reported for information management purposes. **[4-APPFS-3D-31]**

10. At a minimum, quarterly reports from those individuals in charge of the information system and research program are forwarded to the Secretary of Corrections or designee. **[4-APPFS-3D-32]**

11. The Director of Probation and Parole shall receive quarterly reports in accordance with the established format in Policy *CD-010600* (**Management Plan and Quarterly Reporting to Central Office**).

B. CMIS Offender Photos

The digital photos of offenders which are loaded into CMIS shall follow the requirements listed below:

1. Digital Camera should be set to the setting of 640 X 480 resolution & portrait, please refer to your camera operating instructions. The image should not be larger than 300 KB in size for storing the photo to the CMIS system.

2. Offender should stand about six (6) feet from the camera. The offender should take up most of the image in the photo; you may need to use a zoom feature on the camera.

3. A height chart must be behind the offender to adequately show their height on the photo.

4. Offender should be holding a sign reflecting the offender's NMCD number or the offender's NMCD Probation and Parole Offender number, last name, first name and the date the photo was taken using sample format in the **Offender Photo Name Board Sample** Attachment (*CD-044006.A*). There should not be any other information on the board. BLACK INK ONLY. The information must be CLEAR and READABLE.

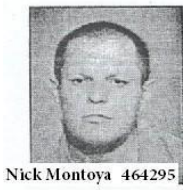
5. Lighting must be adjusted in order for the offender and information to be seen clearly. No reflections from lights or flashes should be in picture.

6. Offender should not be making any hand gestures. (throwing fingers, gang signs, etc… or anything close to them) Remember these pictures also appear on the Corrections Web site.

7. Offender must be clothed.

8. Review the image for clarity and that the image storage size does not exceed 300 KB's prior to storing the photo on the CMIS.

9. If you need to use a photo that you receive from a different area please make sure to add the person's name and offender number as example below:



10. If a photo is not available please use:

C. State Wide Human Resources, Accounting and Management Reporting System (SHARE):

1. The SHARE system is the automated system currently being used by the State of New Mexico which provides complete functional and technical integration across all modules allowing updating and maintenance of a single database for all accounting purposes and human resource functions.

2. The system is centralized at DoIT and connectivity is through a WEB interface.

CD-044007 State Business Social Media	Issued: 08/20/01 Effective: 8/20/01	Reviewed: 5/28/19 Revised: 05/28/19
Alisha Tafoya Lucero, Cabinet Secretary		***Original Signed and Kept on File***

AUTHORITY:

Policy *CD-044000*

PROCEDURES: **[4-4100]**

A. Social Media Types

The types of social media defined by this procedure include, but are not limited to:

1. Social networking sites, such as Facebook;
2. Streaming video and content communities, such as YouTube;
3. Blogs and microblogs, such as Twitter;
4. Virtual gaming.

B. Use of Social Media

Any and all access to social media shall be approved by exception only and must be pertinent to the employee's job or role. Requests must be submitted to the CIO or designee for review and approval prior to access or use.

C. Streaming Video

Any video content that is necessary to view for the purposes of completing valid job duties, training or for approved employee enrichment will be provided to employees via a local area network share, rather than streaming across the internet. Requests must be submitted to the CIO or designee for review and approval prior to local setup and access.

Offender Photo Name Board Sample

NMCD or NMCD Probation / Parole

LAST NAME,

FIRST NAME

NMCD # 00000 or OFFENDER #:

000000

(Date Format) mm/dd/yyyy