| CD-044000 Information Technology Management | Issued: 08/20/01<br>Effective: 8/20/01 | Reviewed: 02/21/25<br>Revised: 02/21/25 |
|---|---|---|
| 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 Expected Practices 5-ACI-1F-01, 5-ACI-1F-02, 5-ACI-1F-03, 5-ACI-1F-04, 5-ACI-1F-05, 5-ACI-1F-06, 5-ACI-1F-07, and 5-ACI-1F-09, *Performance Based Standards and Expected Practices for Adult Institutions*, 5th Edition.
C. ACA Standards 1-CTA-1D-01, *Standards for Correctional Training Academies,* 1st Edition.
D. ACA Standards 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 regard 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. *Artificial Intelligence*: A set of technologies that enable computers to perform a variety of advanced functions, including the ability to translate spoken and written language, analyze data, make recommendations, synthesize human-like responses, create media, and more.

*1)Generative AI (GenAI)*: A set of artificial intelligence technologies that can create new content such as writing, program code, media artifacts, and more using pre-trained models to generate responses from collected data.

*2) Predictive AI:* A set of artificial intelligence technologies that can analyze data to predict future trends or outcomes. Typically uses machine learning techniques to identify patterns in data and make predictions.

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

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

E. *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.

F. *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.

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

H. *Criminal Justice Information (CJI):* Refers to an extensive array of data collected, stored, and managed by law enforcement agencies, integral in ensuring law and order.

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

J. *DoIT:* State of New Mexico Department of Information Technology.

K. *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.

L. *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.

M. *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.

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

O. *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.

P. *HIPAA:* Health Insurance Portability and Accountability Act: An act passed by Congress in 1996 to reform the health insurance industry and ensure workers could maintain health coverage when they change or lose their jobs.

Q. *ICOTS*: Interstate Compact Offender Tracking System

R. *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.

S. *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, regulation, or NMCD policy or procedure. **Proprietary information**, also referred to as a trade secret, 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.

T. *IPR:* Internal Purchase Request

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

V. *Information Technology/Information System*: Computer hardware, software, databases, 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.

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

X. *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.

Y. *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.

Z. *MFA:* Acronym for Multi-factor Authentication, an electronic authentication method in which a computer user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism--knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is).

AA. *PHI:* Protected health information relating to a patient's condition, treatment for the condition, or payment for the treatment when information is created or maintained by a healthcare provider that fulfills the criteria to be a HIPAA covered entity.

BB. *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.

CC. *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.

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

EE. *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.

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

GG. *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.

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

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

JJ. *Virtual Private Network (VPN)*: A method by which a private network is extended and encrypted across a public network that enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

KK. *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.

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

MM. *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.** This policy applies to NMCD employees, contractors and any third parties with access to any agency systems or data, including PHI, PII and CJI, or other sensitive data.

**B.** This policy encompasses all State or NMCD resources, including computers, laptops, tablets, servers, routers, storage devices, software, network, data (including PII, PHI and CJI), 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 devices 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 that allow ITD to create and maintain the appropriate access control mechanisms prior to the collection, storage, retrieval, access, use, and transmission of sensitive or confidential data contained in media format. **[5-ACI-1F-02]**

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.

**C.** 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] [5-ACI-1F-01] [4-APPFS-3D-30]**

**D.** 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]**

**E.** 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]**

**F.** There is a written information technology incident response and management plan to be used in the event that the institution experiences an information technology security breach. The plan is approved by the agency Chief Information Officer or equivalent, reviewed annually and updated as necessary, and is communicated to all staff. The plan includes the following:

- Incident Reporting Procedures
- Staff Roles & Responsibilities for Incident Response and Management
- Incident Investigation Procedures
- Incident Remediation and Closure Procedures
- Post-Incident Review and Action Planning Procedures that Focus on Preventing Future Reoccurrences **[5-ACI-1F-03]**

**G.** The written information technology governance plan shall contain the process by which staff and offender technology assets are identified, obtained, utilized, and maintained in an effective manner to achieve the agency's mission. The governance plan is approved by the CIO, Budget Director and Cabinet Secretary, or designee, and reviewed during the budgeting process and updated each fiscal year as necessary. **[5-ACI-1F-04]**

**H.** This policy shall govern inmate access and use of information technology computing devices. The policy is reviewed annually by the Chief Information Officer or equivalent, updated as necessary, and is communicated to all staff and offenders. **[5-ACI-1F-05]**

**I.** This policy shall govern the issuance, use, and termination of user accounts, the issuance and use of computing devices that connect to the automated information systems, the use of standalone and online applications within the information systems, and the collection, storage, retrieval, access, use, and transmission of sensitive or confidential data that resides in the information system. **[5-ACI-1F-06]**

**J.** All staff that has direct access to information in the information system is trained in and responsive to the system's security requirements. **[5-ACI-1F-07]**

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

**L.** The Secretary shall receive reports concerning research and management information from

those responsible for the management information system. **[2-CO-1F-04]**

**M.** 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]**

**N.** 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]**

**O.** 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]**

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

**Q.** 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 to submit the ITD Information Systems Access form (SAR) for the employee for before access will be granted.

**R.** There is a master index, readily available, identifying all inmates committed or assigned to the agency and/or each institution. **[2-CO-1F-08] [5-ACI-1F-09]**

**S.** 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.

**T.** The use of internet within state 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.

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

**V.** 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.

**W.** 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 HR

**X.** Connecting any computing device not owned by the state of New Mexico to a state network or to any state computing device is prohibited unless authorized in writing by the agency CIO.

**Y.** All remote connections to the NMCD network must have prior approval. VPN tunneling can only be performed from an NMCD device leveraging two-factor authentication. All users must sign the NMCD Telework Access Agreement before remote access is granted.

**AUTHORITY:**

Policy *CD-044000*

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

**A. Computer Systems Access: [5-ACI-1F-07]**

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. Employee managers or supervisors (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 concept of least privilege will be applied for all system access. This concept means giving a user account only those privileges which are essential to perform their duties and intended functions.

7. Contractor(s) 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.

8. 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.

9. The ITD will be immediately notified by the employee's manager or Human Resources 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.

10. 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.

    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 a minimum of eight characters in length, to include an upper and lower case character and either a numeric or special character. The numeric or special character cannot be the first character of the chosen password. 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 six invalid 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. Administrative passwords will be secured and maintained by the ITD.

8. 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.

9. Any employee suspecting unauthorized usage of his or her password privileges must report the suspected unauthorized usage to the Security Officer and have their passwords re-issued.

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

11. Access to computer systems and software will utilize password controls to prevent unauthorized access. It is the responsibility of the employee to make sure that they are properly logged out of any program and the PC is locked at the end of the employee's work day or at any time the employee is away from their workstation for an extended period of time.

12. 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 and the principle of least privilege will also be applied for all administrative or super user access to systems.

13. 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 all IT areas containing sensitive computer systems at all times; only ITD staff members may allow access to restricted IT 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 backups and backup media should be limited to those responsible for handling those tasks.

7. Separation of certain administrative IT duties will be employed and secured through appropriate security, utilizing the principle of least privilege.

8. 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),

9. Violations of access controls must be reported and recorded for review by the CIO or designee, and could result in disciplinary action.

10. Managers and contractor supervisors are responsible for notifying the IT Security Officer, CIO and the Human Resources office concerning persons no longer allowed access to any Agency building for any reason.

11. 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, vocational, or reentry/release 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, 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 periodically and upon request 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, 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 their ID has been established.

5. Data shall not be shared with any outside entity without the review and prior approval of the appropriate Agency administrator, unless such sharing is directed by a policy specific to that data. Further, all data entered into IT systems shall only be utilized for its intended purpose to conduct necessary Agency operations. Staff responding to outside requests to inspect public records under the Inspection of Public Records Act shall make public records available as provided by law, with exempt information redacted and exempt records withheld. Staff responding to public records requests are responsible for coordinating with the appropriate agency administrator as needed to understand when exceptions apply.

**E. Audits:**

1. Audits will be performed on computer system access periodically. Any irregularities will be documented and forwarded to the CIO or designee for review.

2. Procedures will be established and followed to communicate to appropriate parties in the event irregularities are found and to properly remediate any issues found as part of the audit.

3. The ITD's Information Systems Access Security policy shall be read, examined and acknowledged by signature from each Departmental staff member. These forms will be maintained by HR within the employee's personnel file.

**F. Network Management**

1. The agency shall implement a range of network controls to maintain security in its trusted, internal network, and to ensure the protection of connected services and networks. Such controls help prevent unauthorized access and use of the agency's private networks.

2. Separation of duties will be employed to ensure that individuals with operational responsibility for networks shall be separate from those for computer operations;

3. Responsibilities and procedures for remote access to agency resources shall be established.

4. VPN connections to the agency are only permitted from agency-managed VPN devices.

5. The agency's networks shall implement private address routing to public addresses when sending over the internet to minimize the exposure of public routable addresses.

6. Firewall policies shall be configured to accept only inbound and outbound data traffic which is required based on business needs; all other data traffic will be denied. Firewall policies shall take into account the source and destination of the traffic in addition to the content.

7. Details of firewall, and security devices type, software versions, and configuration data will not be disclosed without the permission of the agency CIO.

8. The agency shall define security zones and create logical entities and rules for what comprises permissible data and network traffic between different agency business units.

9. The ITD shall perform network segmentation to control the flow of data between hosts on different segments of the network to provide enhanced security, network performance, and connectivity.

10. The ITD monitors and controls all outbound internet traffic from every networked attached workstation and server via web proxy appliances.

**Form CD-044001.1**
Revised 01/10/2023

**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

**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 all Department employees and contractors, and inmate use, including facility inmate stores, must be approved by the CIO or designee.

2. Acquisitions for new hardware requires the submission of an IPR for review and approval by the CIO or designee prior to purchase.

3. Purchase approval on hardware, new workstations and existing workstations requires that it must meet the minimum baseline workstation configuration. If equipment does not meet these standards, the equipment may not run properly with the identified standard core software suite. This minimum configuration and requirements will be considered as part of the IPR review process by the CIO or designee.

**B. Moving Equipment:**

1. Only authorized ITD personnel may move, transfer or relocate computer equipment and peripherals outside of the office or area the equipment is installed, 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 outside of the general area initially installed should only be necessary when: network access has become breached; access is impossible or otherwise unsafe due to a natural disaster or other qualified direct threat; or Departmental emergency movement or facility relocation. Movement to 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/Malware 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. All external media, including flash drives, DVD's or external hard drive must be scanned by the anti-virus software that has been placed on the computer, 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.

b. New computer acquisitions for any Corrections Division employee or contractor residing on the agency network must include the purchase of licenses for department standard anti-virus/anti-malware software.

c. 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.

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

**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. The Information Technology Division has standardized on Microsoft Office products for office automation purposes, 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 be downloaded through the Internet or installed 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.

   All software purchases requests shall be submitted via IPR for review and approval by the CIO or designee.

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

7. Users and contractors are not permitted to bring software from home and load it into the Department and network computers. Any person loading software without written authorization shall be subject to disciplinary action.

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

9. 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.

10. Only authorized ITD staff may install and configure shareware to work on the computer environment. All compatible shareware software may be considered as an exemption, but should be approved by the immediate supervisor. If the supervisor feels the software should be investigated and deemed as compatible, he/she should contact the ITD for the proper authorization.

11. There shall be a uniform method of collection, recording and organization of software developed for agency 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 infringement 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 maintains workstation standards to assist and aid the various departmental units when acquiring software in their area. These minimum operating standards are considered as part of the IPR review/approval process by the CIO or designee.

2. The New Mexico Department of Information Technology issued the regulations in the New Mexico Administrative Code 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 an IPR form to the ITD to receive permission to purchase or upgrade existing software. All IT purchases shall be reviewed and approved by the CIO or designee.

**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 the CIO.

**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 calendar scheduling and sending/receiving queues of their electronic mail, such as sending an email on behalf of, 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. Transmission of PII or HIPAA Protected Information**

During the course of completing the agency's mission to provide for the safety of employees and inmates, it will sometimes be necessary to communicate or transmit PII or HIPAA-protected data to authorized employees. In the event that this is required, any staff needing to transmit or receive this protected information will utilize the established software and protocol for email encryption. Agency business units and staff that must have this ability

shall purchase and maintain the appropriate licensing.

**E. Record Keeping/Archiving Electronic Mail Messages:**

Any message sent or received that is relevant to the course of business and non-transitory 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 archived periodically according to the number of messages the user receives. DoIT as the owner of the Enterprise email system is responsible for maintaining the current information store for all state employees as well as backing up all electronic forms and messages for a certain period of time. However, it is the user's ultimate responsibility to maintain any email documenting important agency business, in accordance with the state records management requirements for electronic messaging outlined in NMAC 1.13.4. Instructions and assistance in creating offline storage files to archive important messages will be provided by ITD upon request.

**F. Appropriate Use of Mailing List, Discussion Groups and Social Media:**

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.

**G. 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**".

**H. 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 or HIPAA-protected information is redacted and not included in any email communication, unless the appropriate software for email encryption is installed. Some file types are not allowed,

such as applications, zip files, etc., and will be blocked regardless of file size.

If there are difficulties attaching/sending large file attachments, the user will need to contact the ITD for assistance. If the document is being moved from one location to another location within the agency, a network folder will be created instead of email. 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.

An item of note for the above: Even with the outlined process for sending large files, the receiver may also have file size limits for incoming messages or attachments.

**I. Electronic Mail With Corrections Department Attorneys:**

Correspondence to or from any Corrections Department or State-assigned 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.

**J. 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 or CIO.

**K. 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.

**L. Misuse of Electronic Mail:**

Acts considered a misuse of electronic mail and subject to disciplinary actions 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;
- Sending unsolicited bulk mail;
- Sending email containing illegal material such as chain letters involving money or goods;
- Sending email containing material protected by copyright, trademark or trade secrets; and
- Sending email that is considered forbidden by the laws of applicable countries and States.

**M. External Electronic Mail Agents:**

Access to personal Electronic Mail Provider accounts (such as 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.

**N. Operations:**

1. To report any misuse of electronic mail policies, contact the ITD Security Officer or CIO. 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 or CIO. 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 ITD, IT Security Officer or CIO.

**O. Spam/Phishing/Malware**

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, or clicking on embedded links.

1. 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, IT Security Officer or CIO immediately

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. DoIT provides an embedded method within the email system that filters for potential spam. This software notifies an employee via email that messages have been temporarily blocked as potential spam, as well as a method to release the email and either permit or block future emails from the recipient via a personal portal for each email user. Instructions and assistance on how to utilize this portal can be obtained from the ITD.

**P. Multi-Factor Authentication**

The purpose of Multi-factor authentication (MFA) is to curtail and prevent unauthorized access to state resources through either negligent or nefarious means, and is required for all State of New Mexico email accounts. MFA is an electronic authentication method in which

the user must successfully present two or more pieces of evidence (or factors) during the logon process, such as username/password (factor 1) and a pin communicated via a phone SMS message, a call prompt, or a hardware key device (factor 2).

1. MFA authentication administration, maintenance and methods are tied to the Microsoft 365 account provided and maintained by the Department of Information Technology (DoIT).

2. All users with a state-issued mobile device shall utilize that device as their primary MFA authentication method.

3. Any user that is not able to utilize a mobile device or land line phone within their work area will be assigned a key device for the secondary authentication method.

4. Any user that does not have a state-issued mobile device, but is able to utilize a personal mobile or land line phone within their work area may do so.

5. MFA authentication method will be determined based on work location for all new employees as part of the onboarding process.

6. All hardware tokens utilized for MFA authentication will be assigned based on work location and need and will be managed in accordance with the Inventory of Property form (CD-020401.2). Any lost or damaged security tokens will be managed in accordance with CD-020400 Employee Accountability for Department Property.

**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 their 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 email distribution, for off-peak times.

4. Internet permissions are based on job duty and managed through the assignment of appropriate security access. Exceptions to any basic internet permission rule may be granted for a specific business use or need.

**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.

3. All attempted internet access that violates agency or state policies, further outlined throughout this section, will be blocked and logged. Repeated attempts to access prohibited content will result in the revocation of internet privileges for the employee, and the submission of a report outlining the occurrence to the employee's direct supervisor, which may result in disciplinary action.

**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, unless the monitoring of internet activity important to the maintenance of agency security and threat intelligence requires otherwise.

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 must make it clear that they are doing 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, news group, 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 wireless connections to any outside computer or network must be physically isolated from the State's network or protected through a virtual private network (VPN) 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. Approval for this access shall be communicated to the CIO or designee, who will coordinate the granting of access.

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 CIO.

**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 or designee.

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, data, music, movies or any other media.

**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 Google mail, Yahoo, etc. is prohibited over State networks without CIO 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, whether physical or logical (firewall, proxy, Internet address screening program or other security system) will be subject to 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 shall authorize qualified State or contract personnel to perform external penetration testing on firewalls or other network security mechanisms operated by the agency, for the purpose of improving security This testing shall occur on a regularly-scheduled basis.

4. Because the potential exists for some security testing to disrupt operations, the agency's CIO or equivalent must be notified in writing prior to major testing. Where possible, testing will be coordinated to minimize any potential disruption, and will be communicated appropriately to agency staff.

**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 without staff supervision.

2. Inmates may be granted limited access to the Internet to complete educational and vocational programming, or for reentry/release purposes.

3. Inmate access shall be limited to the designated inmate education networks. At no time will the inmate education network and NMCD staff network reside on the same network segment.

4. Instructors, educational staff, and contractors are at no time allowed to provide access to an inmate to an NMCD staff networked computer.

5. Inmates are to only use the designated login credentials provided to them by education staff through the ITD. All inmate access is intended for educational, reentry and programming purposes only.

**AUTHORITY:**

Policy *CD-044000*

**PROCEDURES**: **[5-ACI-1F-01]**

**A. Offender Management Network Information (OMNI): [4-APPFS-3D-30]**

The offender management system (OMS), OMNI, or any other OMS utilized by the agency, 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. The OMS shall be designed, developed, enhanced and maintained to meet the Department's business requirements for managing offenders under NMCD jurisdiction.

2. The OMS 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 and contracted vendor via maintenance and service level agreements.

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

5. The Secretary or relevant Director, Manager or designee shall receive reports concerning research and management information from those responsible for the management information system and research program. **[2-CO-1F-04]**

6. OMS reports will be provided to the agency administrator. Reports may be generated either daily, weekly quarterly, or on-demand, based on specific need and provide the agency administrators summaries of offender population including, but not limited to: offender characteristics, movement and other demographic information. **[2-CO-1F-04]**

7. The OMS will provide a master index identifying all inmates, readily available to agency employees whose duties include offender management, and controlled by security rules.

committed or assigned to the agency. **[2-CO-1F-08]**

8. 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]**

9. 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]**

10. 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. OMS Offender Photos

OMNI provides the ability to store multiple offender photos, both thumbnail and full size, multiple photo types, including front and profile views, scars, marks and tattoos, and photos in support of investigative events. Certain photos may be flagged as sensitive and access controlled based on security rules.

The digital photos of offenders which are loaded into the OMS 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.
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. Distance from the camera for scars, marks and tattoos should be dependent upon the ability to fully see the scar, mark or tattoo and body location identification.

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 NMCD (if inmate) or Probation/Parole ( 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.

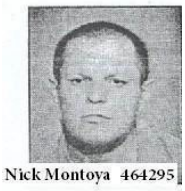
6. Offender must be looking directly at the camera for front photo views.

7. 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.

8. Offender must be clothed.

9. Review the image for clarity prior to upload into OMNI.

**C.** 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:




**D.** If a photo is not available please use:


**E. 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.

**Offender Photo Name Board Sample**

NMCD or Probation / Parole LAST

NAME,

FIRST NAME

OFFENDER #: 000000

(Date Format) mm/dd/yyyy

| CD-044007 State Business Social Media | Issued: 08/20/01<br>Effective: 8/20/01 | Reviewed: 02/21/25<br>Revised: 01/10/23 |
|---|---|---|
| Alisha Tafoya Lucero, Cabinet Secretary | | ***Original Signed and Kept on File*** |

**AUTHORITY:**

Policy *CD-044000*

**PROCEDURES**: **[5-ACI-1F-01]**

**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**

1. 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.

2. Any instance of live streaming from an NMCD workstation must be approved by the CIO or designee.

3. All usage of web conferencing initiated by agency staff will utilize one of the approved web conferencing platforms.

**AUTHORITY:**

Policy *CD-044000*

**PROCEDURES**: **[5-ACI-1F-03]**

**A. Information Technology Incident Management and Response**

The incident response and management plan to be used in the event that the institution experiences an information technology security breach.

1. Reporting of Information Technology related incidents will be performed by informing thIT helpdesk or any member of the IT staff via phone, email or in person. Staff should include their immediate supervisor or manager when reporting IT related incidents.

2. Upon report of an incident to the IT helpdesk or IT personnel, the information regarding the incident is relayed to the IT Chief Information Officer, Deputy Chief Information Officer, and respective IT Manager for further action. Dependent on the type of incident reported, it would be further assigned to the IT Security and Compliance or other appropriate group for investigation and remediation.

3. Assigned IT staff are responsible for working with end-user(s) to determine incident cause and scope of infection or effect.

4. Dependent on incident type (malware infection, email compromise, botnet traffic, etc.) the IT staff assigned to the reported incident will begin by communicating with the affected end-user(s) and begin the process of disabling and/or changing user account credentials as necessary.

5. If the incident deals with an affected computer system(s), the designated IT staff members will begin the process of performing malware and virus scanning using enterprise anti-virus and anti-malware software. If the incident deals with an email account compromise, the assigned IT staff will work with DOIT (Department of Information Technology) to disable user access to the compromised email account. The compromised user account will then be enabled for inspection by IT staff that will check for any infectious or malicious emails, email rules that might have been created as well as changing user account login credentials to prevent further exploitation of account access.

6. After any affected system(s) or account(s) are determined to be remediated, the assigned IT staff handling the incident will compose a report detailing any exploit findings, tasks

performed to complete remediation, and the potential cause of the incident providing it to the IT management team for review.

7. When a report has been provided to the IT management staff, the IT staff handling the incident will work with the affected user(s) to provide education and training on how to better handle any future potential exploits and attempt to prevent future security issues. Furthermore, a generic email pertaining to the incident cause will be sent out to all agency staff explaining the details to look for and actions to take to avoid further security compromises.

8. If it is determined that the infection or exploitation of computer system(s) or user account(s) was of a deliberate and intentional manner, the incident report and further inquiry will be shared with the respective perpetrator's management chain of command for disciplinary action.

**AUTHORITY:**

Policy *CD-044000*

**PROCEDURES**: **[5-ACI-1F-04]**

**A. Information Technology Governance**

The process by which staff and offender technology assets are identified, obtained, utilized, and maintained in an effective manner to achieve the agency's mission.

1. A process or need is identified by NMCD staff in a request to the Information Technology Division for assistance with improving or simplifying their current business process.

2. An IT assessment will be performed by the appropriate IT staff to determine the necessary hardware or software technology needed to accommodate the end user's needs. Technical research is performed to ensure compatibility with existing software applications and hardware peripherals. This assessment may result in the purchase of new hardware or software, and may require a new project and/or funding request in accordance with CD policy-044200 IT - Project Management.

3. When a necessary hardware or software platform is identified, the information technology staff will work with vendors to obtain bids ensuring competitive pricing and providing the requesting division the best available cost. The IT Staff must perform due diligence in leveraging vendors on a state-wide price agreement when possible, ensuring the best value to the agency.

4. All computer equipment is to be delivered to the Information Technology Division located at the New Mexico Corrections Department Central Office in Santa Fe or the IT Office at the Charles S. Gara building in Albuquerque, as determined by ITD. All equipment sent to/ received by IT staff. Inventory, imaging, and configuration will be performed by the designated IT staff members prior to deployment and distribution on the NMCD network. The process will ensure compatibility and proper functionality for all newly purchased IT equipment. In the instance that equipment is found to be defective or incompatible, the IT division will work with the vendor to obtain a replacement.

5. All software downloads and installations are to be performed by IT Staff only.

6. Computer hardware and peripheral installations requiring administrative rights are to be performed by IT staff only.

7. All new desktop and laptop equipment are inventoried through the department's online asset

management system. The system tracks a full asset inventory including make, model, and serial number. The system provides a full software inventory of all loaded programs.

8. All NMCD IT equipment is to be maintained with the latest firmware updates, software versions and security patching to ensure protection from any known vulnerabilities.

9. All IT equipment intended for use by the inmate population will be configured, and maintained by the ITD. All technology equipment used for inmate education, programming, visitation or any other approved use shall be configured in a secure manner limited access to only the necessary functionality for its intended purpose.

10. User accounts configured on any inmate devices are to be administered by IT staff only. Educational instructors are to work directly with IT staff on any requests for software installations and programming changes.

11. All NMCD network credentials and user accounts are to be administered by IT staff only.

12. Network file shares, folder permissions, and network folder creation is to be performed and administered by NMCD IT staff only. Requests for the creation of new network folders is to be approved by the IT CIO or designee. Certain sensitive folders or network locations will be further secured and maintained solely by the CIO and Deputy CIO or designee.

13. The issuance of any new IT equipment to be used by NMCD staff or the inmate population will be performed and vetted by NMCD IT staff only.

**AUTHORITY:**

Policy *CD-044000*

**PROCEDURES**: **[5-ACI-1F-04]**

A. **Mobile Device Usage**

1. The responsibility for the appropriate use of mobile devices rests with each designated or authorized NMCD user. NMCD's Cabinet Secretary or designee and CIO are responsible for providing relevant information regarding policies and procedures to NMCD users who in turn are responsible for reading and abiding by the provided rules and policies upon receipt of a mobile device.

2. NMCD users shall have no expectation of privacy regarding use of State issued mobile devices including but not limited to installed apps, multimedia use, downloads, data stored on the mobile device, usage, or messages in any form received or sent via the mobile device.

3. All mobile devices are the property of NMCD, and the State of New Mexico and they are intended only for each employee's legitimate business use. Any alteration of a mobile device's operating system or the attempted removal from the agency's Mobile Device Management system is prohibited. Users shall do all that is reasonable and necessary to ensure that no NMCD issued mobile device shall be "Jail Broken" or "Rooted" by anyone.

4. As property of NMCD or the State of New Mexico any apps installed on the mobile device should not be through the user's personal account, i.e., an iTunes account, g-mail account, etc Where such an account is required for State of New Mexico business, separate accounts associated with the employee's state email shall be approved by the employee's direct supervisor, reporting Bureau Chief and CIO, and created by NMCD's ITD.

5. Incidental personal use is acceptable provided it does not interfere with state business and is consistent with applicable State or Department policies and rules. NMCD has the authority to limit personal or incidental uses on any Department owned mobile device.

6. NMCD users shall not use, try to use, or let anyone else use mobile devices for: anything that is illegal; making offensive, threatening, or harassing calls; or messaging or emailing inappropriate or offensive remarks, graphics, or images. NMCD staff for whom the device was purchased or acquired shall be accountable for any inappropriate use of the mobile device.

7. A Specific NMCD employee name must be associated with every mobile device. For a

"floater device", a manager or direct supervisor's name must be associated with that mobile device.

8. Mobile devices shall not be allowed into any NMCD prison facility without the prior approval of the facility Warden and CIO.

B. **Mobile Device Security**

1. Mobile devices shall only be used by authorized NMCD employees. Internet, Intranet, Email and Digital Network usage rules; enterprise security policies and rules, NMCD code of conduct policy, and State or Department personnel rules apply to the use of all mobile devices.

2. Only DolT, or NMCD ITD on behalf of DolT, has the authority to install software to secure mobile devices consistent with the policy and ensure appropriate State business usage.

3. All mobile devices must be password-protected. Each device must be set to lock no later than (5) five minutes of inactivity.

4. To the greatest extent possible, confidential, privileged, or sensitive information, client date, or other information as covered or referenced by existing state or federal privacy or confidentiality laws, regulations, rules, policies, procedures, or contract terms should not be stored on mobile devices. Sensitive information, if stored on mobile devices, shall be secured, and shall be encrypted. Sensitive and critical data or information stored on a mobile device shall not be the only instance of data. Additionally, sensitive information must be transmitted in a secure fashion.

5. Mobile devices must be securely stored when not in use. Mobile device screen protectors should be used to provide a degree of physical protection and may be requested. Users may be liable for repair or replacement costs, should an NMCD issued mobile device be damaged or lost.

6. All broken, damaged, or malfunctioning mobile devices must be reported to the employee's direct supervisor and reporting Bureau Chief for replacement or repair.

C. **Mobile Device Procurement**

1. Only mobile devices and services listed on the DolT Service Catalog are available to NMCD employees.

2. All requests for the procurement of mobile devices and services available through the DolT Service Catalog must be approved by NMCD's CIO and submitted to DolT for processing through NMCD's Telecom Coordinator. Additionally, all requests for change to any mobile devices and/or associated services provided through DolT must be approved by the individual's supervisor, Bureau Chief and CIO, and shall be submitted to the NMCD Telecom Coordinator.

D. **Mobile Device Management**

1. All applicable agency provided mobile devices must be configured and provisioned utilizing the agency's Mobile Device Management platform by NMCD ITD personnel prior to deployment and use. The provisioning of newly acquired mobile devices or existing non-provisioned mobile

devices must be coordinated with NMCD ITD.

2. The mobile device provisioning process requires that NMCD ITD be provided with the serial number(s) of the mobile device(s) needing to be provisioned for submission to DOIT. The mobile device provisioning process is dependent on user data needs.

3. New, replacement, or otherwise unconfigured devices with no user data will be erased and configured by the agency's MDM solution without data backup efforts. Existing non-provisioned mobile devices in current use by staff will require a "best attempt" data backup effort prior to erasing and configuring the mobile device by the agency's MDM solution. Once the mobile device has been configured, the backed-up user data will be restored to the mobile device. Due to limitations of the provisioning processes and backup solutions available, all user data back up efforts are "best attempt".

4. Very sensitive data may be stored on a mobile device. Therefore, the loss of a mobile device that can send, store, and retrieve email or access DolT or State information systems has potentially serious repercussions for the State. All missing, lost, or stolen mobile devices must be immediately and formally reported to the employee's direct supervisor, reporting Bureau Chief, NMCD's CIO and NMCD ITD Helpdesk which will then notify the DoIT service desk. The mobile phone number for a missing lost or stolen phone will be immediately disabled and any mobile device provisioned through the MDM solution will be remotely disabled or erased.

**AUTHORITY:**

Policy *CD-044000*

**PROCEDURES**: **[5-ACI-1F-04]**

A. **GenAI Usage**

1. Any use of or development with GenAI applications, content or tools must be consistent with NMCD policy, code of conduct, acceptable use, state regulations and any applicable law.

2. As with all software and applications, the use of GenAI applications or products must first be approved by and requested through an employee's supervisor/chain of command, for review by the CIO or designee.

3. Employees, contractors and system/data users are prohibited from using or attempting to gain access to unapproved GenAI applications or websites when:
   a. Using NMCD systems, devices, or networks,
   b. Conducting business on behalf of NMCD,
   c. Using NMCD data.

4. Use of any application that utilizes predictive artificial intelligence is strictly prohibited without agency approval, purchase and established scope or purpose.

5. Example of acceptable use and acceptable use cases/disposition of GenAI:

| **Acceptable GenAI Application** | |
|---|---|
| ChatGPT | |
| | |
| **Acceptable Use Case** | **Disposition** |
| Translating text from a secondary, publicly available source | Acceptable |
| Conducting high-level background research into a non-sensitive topic | Acceptable |
| Summarization of documents not containing any PII, PHI, CJI or sensitive NMCD data. | Acceptable |
| Using agency assigned credentials to log into publicly available GenAI application | Not acceptable |
| Storing history or agency data to help a | Not acceptable |

| **Acceptable GenAI Application** | |
|---|---|
| ChatGPT | |
| | |
| **Acceptable Use Case** | **Disposition** |
| publicly available AI "learn" | |

B. **GenAI Security**

1. In order to prevent potential security incidents or data leaks:
   a. Do not use agency credentials, email addresses, or phone numbers as a login to publicly available GenAI applications,
   b. Do not install non-approved Application Programming Interfaces (APIs), plug-ins, connectors, or software related to GenAI systems,
   c. Do not implement or use in any way code generated by GenAI on NMCD systems.

2. In order to maintain the confidentiality of NMCD sensitive information, employees, contractors, or third parties with access to sensitive NMCD information must not share information with non-approved personnel and must not input sensitive information into any GenAI systems. Specifically:
   a. Do not input Intellectual Property (IP) into GenAI applications.
   b. Do not enter Personally Identifiable Information (PII) into GenAI applications.
   c. Do not enter Personal Health Information (PHI) into GenAI applications.
   d. Do not enter Criminal Justice Information (CJI) into GenAI applications.
   e. Follow NMCD data handling policies.

3. NMCD reserves the right to access and monitor the use of GenAI applications on agency-issued devices or when accessed through agency-managed networks, or when involving agency data to ensure the compliant use of these systems.

4. Employees who fail to comply with any provision of this policy may be subject to discipline up to and including termination. Violations by contractors may be considered breach of contract and result in removal from assignment. Any GenAI-related activities which appear to violate applicable laws will be reported to external law enforcement.

C. **Ethical Use of GenAI**

1. To protect employees from harm and NMCD from reputational, monetary, and legal damage, employees must use approved GenAI pursuant to NMCD and NMAC code of conduct and non-discrimination policies.

2. GenAI-created content that is inappropriate, discriminatory, or otherwise harmful to employees, offenders, contractors, third parties and people living in New Mexico must not be utilized for work purposes.

3. To ensure the ethical use of GenAI:

a. Review all output of GenAI applications to make sure it meets NMCD standards for equity, ethics, and appropriateness.

b. Do not use any output that discriminates against individuals on the basis of race, color, religion, sex, gender identity, sexual orientation, national origin, age, disability, marital status, political affiliation, genetic information, or any other established protected class.

c. Do not use GenAI applications to create text, audio, or visual content for purposes of committing fraud or to misrepresent an individual's identity.