

Information Technology Use, Revision 2

Source Document:	IS-1002
Release Date:	10/2/97
Revision 1:	2/25/04
Revision 2:	11/22/04
Responsible Department:	Administration
Reference Material:	Employee Handbook, CNM Handbook 12.17 Student Handbook Family Educational Rights and Privacy Act 1974 Governing Board Policy Handbook 9.03
Support Material:	3-Step Response to Tech Use Violations Technology Use Violation Matrix
Forms:	Information Technology Use Violation Report

CNM Board Policy

Employee Handbook 12.17, CNM Technology Use Policy

Administrative Directive

Contents

Purpose

Information Technology at CNM

1. Promotion of Information Technology Use
2. Administration of CNM's Resources and Systems
3. CNM Enterprise Resources and Systems

Technology Use

4. Information Technology Users
5. Agreement and Compliance
6. Dissemination of User Information
7. Rights and Privileges
8. College Liability
9. User Liability
10. Authorized Use
11. Responsible Use
12. E-mail and Internet Use
13. Personal Use

System Access

14. Access and Eligibility
15. E-mail and Web Accounts
16. Locking Accounts
17. Disruption of Service
18. CIT Customer Support Center

System and User Protection

19. Monitoring
20. Privacy
21. Preserving Information
22. Intellectual Property
23. Inappropriate Material

Information Technology Use Controls

24. Reporting a Violation
25. Enforcing this Directive
26. Information Technology Use Violations
27. 3-Step Response to a Violation

Definitions

28. Definitions

Purpose

Central New Mexico Community College (CNM) promotes and provides Information Technology (IT) resources that enhance educational services and facilitate job performance and College operations. These resources are shared by students, faculty, staff, and the public. All persons using these systems share the responsibility for seeing that they are used in an effective, efficient, ethical, and lawful manner. The aim of this administrative directive is to safeguard equipment, networks, data, and software that are acquired and maintained with public funds as well as define the acceptable use of these resources.

Users of CNM technology resources, including those who interface with CNM systems and networks, are subject to this administrative directive, in addition to local, state, and federal laws relating to copyrights, security, and other issues regarding electronic media. Any violation of this CNM policy, administrative directive, the Employee Handbook, or the Student Code of Conduct may result in the removal of access privileges and subject the violator to administrative and disciplinary action. Examples of Information Technology Use violations are listed on the Violation Matrix.

Information Technology at CNM

1. Promotion of Information Technology Use
2. Administration of Resources and Systems
3. CNM Enterprise Resources and Systems

This administrative directive applies to all individuals and groups utilizing College-owned Information Technology resources, whether individually controlled or shared, stand-alone or networked.

1. Promotion of Information Technology Use

CNM encourages students, instructors, and employees to make use of Information Technology resources. To support this intent, CNM provides computer access at several computer labs throughout the College and offers a variety of computer-related courses. Please check with the individual labs for hours of operation and the category of users they serve.

Courses and workshops on computer use and Information Technology are available at CNM to students and employees through the following departments:

- College of Arts and Sciences
- Technologies
- Business Occupations Department (BOD)
- Health Occupations
- Trades & Services Occupations
- Learning Resources Center (LRC)
- Adult and Development Education – (DADE)
- Workforce Training Center (WTC)
- Emeritus Academy

- The Teaching and Learning Center (TLC) – employees only
 - 1.1 Instructors are encouraged to assign projects and homework that require the use of computer technology. This gives the student an opportunity to prepare for jobs and continuing education as well as partner in the protection of CNM’s Information Technology resources. Instructors should provide an explanation of student responsibilities and encourage students to read the Information Technology Use Administrative Directive which also provides links to CNM Governing Board Policy.
 - 1.2 Employees are encouraged to become familiar with and use the Information Technology resources at CNM. Employees can enroll in CNM courses and workshops. Workshops are also available through the Teaching and Learning Center. These workshops are designed for instructional staff but are open to other CNM employees if space is available. Tuition waivers are available to eligible individuals.
 - 1.3 CNM encourages every student and employee to have a current account, to promote student-faculty dialogue and timely response to business-related communication among the CNM community. CNM accounts are available to eligible individuals.

2. Administration of CNM’s Enterprise Resources and Systems

In support of CNM’s mission to provide dynamic education for the community, the College has charged CNM’s Computer Information Technology (CIT) Department with the responsibility of maintaining the capacity, performance, security, and stability of CNM’s Enterprise resources. To accomplish this and ensure maximum availability of computing resources, the following applies:

- 2.1 All systems attached to CNM's networks, including those not administered by CIT are required to adhere to this, and any other applicable administrative directives, as well as processes, procedures and best practices necessary to maintain the integrity of CNM’s systems and networks.
- 2.2 Prior to the purchase of new hardware or software, it is recommended that CIT be involved early in a project to review and assess compatibility issues with respect to special or unique systems and applications for departmental, group or individual use.
- 2.3 All new systems, and changes to or deletions of existing systems attached to CNM's networks, are subject to review and approval by CIT. If necessary, appeals to CIT decisions can be made through the Information Technology Strategic Team (ITST).

3. CNM Enterprise Resources and Systems

This administrative directive governs and protects all communication and computer resources utilized by the CNM community.

Information Technology systems at CNM consist of enterprise applications, services, and equipment. The categories and items listed below provide a general overview of the most common resources in use at CNM.

Computer Systems	Voice Communication Systems
Desktops Servers Laptops – including wireless portable labs Software Web Systems and Services (Inter, Intra & Extra) Enterprise servers Storage systems	Desktop telephones Telephone systems (internal & external) Voicemail Facsimile machines Compression technologies Digital transport systems (bandwidth) Cellular telephones PDA's (Personal Data Assistant Devices) Combination PDA – Cellular telephones
Networks	See IS-1004 Cellular Telephones and IS-1006 Laptops for further information regarding these devices.
Microwave Routers, switches, hubs, repeaters Wireless networks Cable infrastructure Digital transport systems (bandwidth) Compression technologies Remote access	
Applications	Internet Services
Listservs Chat rooms Conferencing systems E-mail Calendaring systems Banner and Associates interfaces Web applications and systems STARS Voice Response systems Administrative Operating systems	Infrastructure Cable modems Microsoft domains Web domains Internet Service Provider (ISP) Internet Service Provider modem connections Dynamic Host Configuration Protocol (DHCP) Domain Name Service (DNS) Windows Internet Naming Services (WINS) Active Directory Service (ADS) Digital Subscriber Line (DSL) Virtual Private Network (VPN) Remote Access Server (RAS)

Technology Use

4. Information Technology Users
5. Agreement and Compliance
6. Dissemination of User Information
7. Rights and Privileges
8. College Liability
9. User Liability
10. Authorized Use
11. Responsible Use
12. E-mail and Internet Use
13. Personal Use

4. Information Technology Users

- 4.1 By using any of CNM's resources and systems, users agree to familiarize themselves with, and accept the terms of the Information Technology Use Administrative Directive.
- 4.2 The individuals and groups who are governed and protected by this directive include, but are not limited to:
 - students, including those enrolled in distance learning classes
 - faculty
 - staff
 - organizations with websites and e-mail addresses
 - departments with websites and e-mail addresses
 - general public (limited access in designated areas)
 - authorized business partners
 - authorized vendors/contractors
- 4.3 The general public, while using CNM resources and systems, are subject to all applicable CNM policies, administrative directives, and procedures.

5. Agreement and Compliance

The aim of this agreement and compliance is to ensure that CNM's Information Technology resources and systems are used in an appropriate manner. Agreement and compliance with this administrative directive ensures that the CNM community has optimum access to and use of these resources.

- 5.1 Information Technology standards, directives, and requirements must be in compliance with this administrative directive so that all processes support the integrity of CNM's resources and systems. Users agree to abide by this administrative directive for systems, networks, or services that they may access through CNM's systems.

- 5.2 Area directives and procedures may be established to further support appropriate Information Technology use to preserve all resources and better serve the community. Users agree to become familiar with and to abide by all applicable directives in addition to the Information Technology Use administrative directive.
- 5.3 The CIT Support Center and/or the Policies and Procedure Office staff are available to explain or interpret the information contained in this administrative directive or other applicable area directives that may need clarification.

6. Dissemination of User Information

Institutional leadership is encouraged to make every reasonable effort to make the information contained in this CNM policy and administrative directive available to students, employees and the public. By logging into any of CNM's networks or applications, users agree to comply with this administrative directive. However, it is recommended that users read the CNM Information Technology Use Policy and Administrative Directive to fully understand their rights and responsibilities.

- 6.1 Information may be conveyed in various ways, some of which are:
 - hand-outs
 - presentations at staff meetings
 - presentations at New Employee Orientation sessions
 - presentations at New Student Orientation sessions
 - informal training sessions conducted at the department level
 - official CNM publications (e.g., Course Catalogue)
 - wall postings in the computer labs
 - screen messages that require "user acceptance of policy" to log on
 - website(s)
 - e-mail

7. Rights and Privileges

CNM and the users of CNM's Information Technology resources and systems have certain rights that are in place to safeguard both the College and the CNM community. These rights are not intended to be in conflict with each other, but rather to promote a reciprocal relationship between the administrators of CNM's Information Technology resources and their users.

Rights of CNM

- 7.1 CNM's Information Technology resources and systems are owned and operated by CNM. These resources include systems, networks, software/licenses, facilities, accounts, and information. CNM reserves all rights to these resources, including termination of service without prior notice should an individual violate CNM's Information Technology Use Administrative Directive. CNM further reserves the right to review all software and files maintained on CNM's computers.

Privileges

- 7.2 Access to CNM's resources and systems is a privilege granted to users, not a right. Access privileges are offered to users so they have full use of the technology available for academic or CNM work-related purposes. Access to any system may be denied or revoked at any time without prior notice as a protective measure to ensure CNM's system integrity or compliance with legal mandates.
- 7.3 Users may not, under any circumstances, transfer or confer these access privileges to other individuals.
- 7.4 Access privileges to CNM's Inter/Intranet require responsible behavior by users and their compliance with the Information Technology Use Policy.
- 7.5 Access privileges may be temporarily suspended, if necessary or appropriate, to maintain the integrity of CNM's systems or networks.

8. College Liability

CNM's role in managing Information Technology resources and systems is to administer and support CNM's Information Technology resources and to facilitate the transmission of data. However, CNM's liability is limited by the following:

- 8.1 CNM does not represent or warrant that any computers or software supplied by CNM will function or perform to any specifications.
- 8.2 CNM cannot protect individuals against the receipt of material that may be offensive to them while they are using the College's resources and systems.
- 8.3 The user is solely responsible for the message transmitted and may be subject to disciplinary action should the transmission be in violation of this directive.
- 8.4 CNM is not responsible for monitoring transmissions for compliance with this administrative directive or any applicable state or federal law. However, when warranted, CNM may elect to monitor electronic communications and activity.
- 8.5 CNM is not responsible if a user's data becomes corrupted or is lost. Locally stored data is not backed-up by CIT (i.e., data/files stored on user's PC hard drives). It is advisable that users back-up data they consider critical to their academic work, job or intellectual property, using modern procedures. CIT provides assistance with back-ups of data on a routine basis as requested. Contact the CIT Support Center for assistance with establishing a back-up routine if needed.

9. User Liability

- 9.1 Users are responsible for backing-up data they consider to be critical to their academic work, job, or intellectual property.
- 9.2 Users are solely responsible for any messages transmitted with CNM's resources and systems. Users may not send messages which are intended to mislead the recipient by suggesting that the message originated from a source other than the person transmitting the message. Further, messages should be appropriate only for a learning environment. Should the transmission be in violation of this administrative directive, the user may also be subject to disciplinary action.
- 9.3 A user who violates intellectual property law may be liable to the owner for actual damages, statutory damages, profits, court costs and attorney fees. In addition, in certain cases the user may be criminally prosecuted and subject to a fine and imprisonment.

10. Authorized Use

CNM authorizes the use of its Information Technology resources and systems, per the account eligibility requirements, for the following:

- academic pursuits
- dissemination of information
- research (e.g., grants, contracts, course-related work)
- educational services (e.g., instructor websites, WebCT, testing, special services)
- operational purposes (e.g., payroll, purchasing, student registration)
- management purposes (e.g., CNM Express, The Source)
- communications-(e-mail, web, telecommunications, distribution and group lists)

11. Responsible Use

Prudent and responsible use of Information Technology resources and systems begins with common sense and includes respecting the rights and privacy of other users.

- 11.1 Responsible use of CNM Information Technology resources and systems includes, but is not limited to the following:
 - proper use of the system per the information provided in this administrative directive
 - proper use of hardware (e.g., not abusing or misusing keyboards, mice, etc.)
 - compliance with this administrative directive and other applicable College policies and administrative directives as well as processes, procedures and best practices identified by CNM to be necessary to maintain CNM's resources and systems
 - use of CNM resources and systems in a manner that respects the privacy of others

- protection of CNM's resources and systems by not engaging in any prohibited or illegal activities (link to the Violation Matrix)
- protection of their user accounts and data (i.e., password protection, not leaving unattended any device they are logged into, backing up critical data)
- proper use of their access to Information Technology resources and systems (i.e., not using it beyond the scope of the job duties they are assigned)
- keeping information/data confidential as required by the user's position or relationship to CNM

12. E-mail and Internet Use

- 12.1 The same standards of behavior and etiquette are expected in the use of e-mail, web, and internet tools as in the use of telephones, written and oral communication.
- 12.2 The items listed in the Example Violations matrix apply to the transmission and content of e-mail, web, or other internet communication tools.
- 12.3 CNM reserves the right to take measures to protect the integrity of its Information Technology resources and systems. Such measures may block the receipt of executable files, detect known viruses, and prevent excessively large file attachments from interfering with system and network operation. However, CNM makes every reasonable effort to preserve the content of electronic communications impacted by these measures.
- 12.4 Electronic mail lists (personal, public distribution or group lists) are for academic or CNM work-related use.
- 12.4.1 Users of an electronic mail list are responsible for determining its purpose before sending messages to, or receiving messages from, the list.

13. Personal Use

CNM allows incidental personal use of Information Technology resources and systems such as telephones, e-mail, and the Internet, as long as it does not adversely affect the College, an employee's job performance, or other users' access to resources.

- 13.1 Personal use of Information Technology resources and systems should be kept to a minimum as determined by individual department managers, supervisors, and instructors. Should such use become disruptive to CNM's system or network operations, the user's access may be terminated without notice to preserve system integrity.
- 13.2 Personal use of these resources and systems may be curtailed by a supervisor if such use impacts an employee's job performance.
- 13.3 Supervisors and managers determine, in concert with this directive, what is acceptable regarding the use of personal items such as cellular telephones, PDA's, and laptops.

System Access

14. [Access and Eligibility](#)
15. [E-Mail and Web Accounts](#)
16. [Locking Accounts](#)
17. [Disruption of Service](#)
18. [CIT Customer Support Center](#)

14. Access and Eligibility

Access privileges fall into four categories – account access, network/system access, access to computer labs, and library resources. Access privileges and eligibility are based on the user’s relationship to the College.

- 14.1 Account access is limited to systems which allow users to perform specific functions, (e.g., e-mail accounts, Banner accounts to perform payroll functions, student registration, or entering grades).
- 14.2 Network/system access can be via Intra/Internet, allowing access to multiple systems (e.g., the Internet and file storage systems).
- 14.3 Access to most computer labs is restricted to certain user populations.
- 14.4 Library facilities are available to all users, but some specific resources are limited to certain user populations.

Account Access Privileges

- 14.5 Access privileges to CNM Information Technology resources and systems are assigned and managed by the administrators or persons designated for managing access to systems.

Account Eligibility

- 14.6 To be eligible for a CNM account, an individual or group must be one of the following:
 - a CNM student
 - a CNM staff
 - a CNM instructor
 - a CNM department
 - a CNM organization
 - an individual (contractor, vendor, etc.) or entity approved by the CNM Vice President for Administrative Services and the Director of CIT

Account Management

- 14.7 Because account access is granted on an individual basis for educational and CNM work-related purposes, usernames and passwords are used to access CNM's resources.
- 14.8 Users are required to log off any device before leaving the area to prevent unauthorized access by others.
- 14.9 CNM accounts must not be used or constructed in a manner that allows any unauthorized access to CNM's resources.
- 14.10 Accounts residing on, or accessing CNM's resources and systems must conform to copyright law (link to Intellectual Property section).

Revocation or Denial of Access Privileges

- 14.11 Access to resources and systems may be denied or revoked at any time without prior notice to protect and preserve system integrity.

15. Computer User Accounts

CNM offers a variety of computer accounts including, but not limited to, portal, email, and web accounts.

- 15.1 Portal accounts (CNM Passport) are automatically created for all students, staff, and faculty.
- 15.2 Student portal groups are subject to approval by the Dean of Students Office.
- 15.3 Employee portal groups may be created for official CNM business and are subject to approval as follows:

Interdepartmental Faculty Groups - Vice President for Instruction or designee

Intradepartmental Groups - Department Dean/Director or designee

Quality Improvement and AQIP Teams - Associate Vice President for Instruction or designee

Divisional Groups - Vice President for the Division or designee

Institutional Groups - Dean/Director of the Group Leader

- 15.4 Websites must conform to CNM's Web Administrative Directive available on CNM's website via [The Source](#). Hard copies of The Source are available from all campus libraries. Any questions regarding Web Policy should be directed to the [CNM Webmaster](#).

16. Locking Accounts

There are times when events, such as employment separation or a suspected violation of this administrative directive, may necessitate the locking of a user's account to preserve and protect the integrity of CNM's systems and networks.

Employee Accounts

- 16.1 Accounts are locked upon termination of employment at CNM. It is the supervisor's responsibility to ensure that the separation checklist is processed through CIT on the same day of the employee's separation from the College.

If an employee's termination results in insufficient time to complete the separation checklist before they leave the College, Human Resources can notify CIT via e-mail to lock the employee's account. However, the separation checklist should be completed as soon as possible.

- 16.2 Upon separation from the College, an employee's data and system files are, and remain, the property of the College.
- 16.3 Information contained in each locked account is kept for a period of no less than thirty days. At the end of that period, the information may be retained or deleted at the College's discretion and in accordance with state statutes and codes regarding record retention.
- 16.4 Access to information in an employee's, or separated employee's locked account requires approval from the Human Resources Department.
- 16.5 Any employee whose account is locked as a result of a suspected violation of the Information Technology Use Administrative Directive is notified by the Human Resources Department.

Student Accounts

- 16.6 Student accounts are kept active until the beginning of the next fall or spring term following their last enrollment. At that time, if the user is no longer a registered student, the account is locked.
- 16.7 Information contained in the account will be kept until the end of the term in which the account was locked and then archived for the duration of the next fall or spring term. If, by the end of that term, the account has not been re-activated due to re-enrollment, the information in the account will be deleted.
- 16.8 Access to information in a student's locked account requires approval from the Office of the Dean of Students.

- 16.9 Any student whose account is locked as a result of a suspected violation of the Information Technology Use policy is notified by the Office of the Dean of Students.

17. Disruption of Service

It is the responsibility of CIT, and/or departmental staff that provide support, to ensure proper notification to individual users and the CNM community at large of any actions that would impact the use of institutional Information Technology resources and systems.

Emergency

- 17.1 Emergency outages of network and computer systems occur on occasion due to hardware or software problems, viruses, and/or performance issues.
- 17.2 The CIT Support Center notifies impacted users of emergency outages, via e-mail or the Voicemail Broadcast System.

Non-Emergency

- 17.3 CIT makes every reasonable effort to minimize disruptions of service to Enterprise Information Technology resources and systems by scheduling routine maintenance and repair during times when fewer users are utilizing them.

Examples: Software or hardware upgrades and installations; transferring data from one server to another; relocating data communication lines, etc.

- 17.4 The CIT Support Center notifies impacted users of planned outages to Enterprise Information Technology resources and systems a minimum of three business days in advance, via e-mail.
- 17.5 CIT can facilitate notification of planned outages for non-Enterprise resources and systems upon request.

Other Disruptions To Resources and Systems

- 17.6 If technical problems are experienced with CNM computer hardware or software, contact the CIT Support Center for assistance at 224-4357.
- 17.7 Report detected or suspected viruses on PCs or networks to the CIT Support Center immediately at 224-4357.

18. CIT Support Center

CIT provides advisement, consulting, hardware and software installation, and support services for users of CNM's Information Technology resources and systems.

- 18.1 For questions and information regarding CNM's Enterprise Information Technology resources and support, contact the CIT Support Center at 224-4357, or visit the CIT website.

System and User Protection

19. Monitoring
20. Privacy
21. Preserving Information
22. Intellectual Property
23. Inappropriate Material

19. Monitoring

Inspections

- 19.1 CNM does not routinely monitor transmissions, files, or data. However, to protect CNM and the community, CNM reserves the right to monitor transmissions, files or data , if a student or employee Code of Conduct or legal violation is suspected, or for other just cause.

Audits

- 19.2 Audits are prompted by compliance concerns that threaten CNM systems, networks, or individual users. Audits of transmission files or data stored on CNM systems and networks may be required in response to investigations regarding threats to the CNM community (i.e., students, employees, and general public), compliance issues, flaws in work practices and/or when mandated by state legislation or school policy.

Investigations

- 19.3 If there is evidence or suspicion of a violation of this administrative directive or any other CNM policy or applicable law, written authorization may be given by the Human Resources Department or the Office of the Dean of Students to do a system audit and inspection. If an investigation is necessary, the user, when requested, will cooperate fully with the investigation.

20. Privacy

CNM makes every reasonable effort to ensure the security of its systems and networks. While attempts have been made to ensure the privacy of all accounts by assigning individual PINs and passwords, CNM offers no guarantee or representation that any account, electronic mail, or voice mail is private. Users should also note that CNM's systems and networks are not guaranteed to be secure. However, CNM does secure sensitive information such as credit card and/or social security numbers entered for Online Registration through the use of encryption software.

There are several internal and external factors that can impact user privacy: federal and state law, protocol intrinsic to computing technology, and standard practices.

Federal and State Law

Personally identifiable information, as well as certain information pertaining to students is protected by state and federal laws.

The following federal and state laws, although not an all-inclusive list, provide additional information regarding privacy.

- Electronic Communication Privacy Act of 1986 (ECPA)
- Gramm-Leach-Bliley Act of 1999 (GLBA)
- Family Educational Rights and Privacy Act of 1974 (FERPA)
- New Mexico's Inspection of Public Records Act (Section 14-2-1 NMSA 1978)
- Confidential Materials Act (Section 14-3(A)-1 NMSA 1978)
- The US Patriot Act
- Exceptions to the ECPA can be found at this link "Privacy in Cyberspace," (<http://www.privacyrights.org/fs/fs18-cyb.htm>)

Protocol Intrinsic to Computing Technology

In the course of performing routine operations and maintenance, as well as in adherence to procedures to secure CNM's Information Technology resources and systems, systems administrators and other authorized personnel have access to user data and account information. It is incumbent on such personnel to protect the privacy of all user data and account information.

The type of information accessed during routine operations and maintenance can be found at this [link](#). (see Resource page at the end of this document).

Standard Practices

It is an expectation of all users of CNM's Information Technology resources to ensure the privacy and confidentiality of past, present and future members of the CNM community.

Users of CNM's Information Technology resources and systems share the responsibility for keeping their own and the College's data private and secure through standard practices (see Resource page located at the end of this document) that support Information Technology use at CNM.

21. Preserving Information

With the steady advancement and use of Information Technology and the move toward electronic records and record storage, CNM is increasingly dependent on the accuracy, availability, and accessibility of information stored electronically and on the computing and networking resources that store, process, and transmit this information.

- 21.1 CNM complies with State records retention codes and regulations. Some departments within the College may have longer retention schedules that exceed state requirements.
- 21.2 Requirements for the retention of electronic records (employee files, student records, and business files) are the same as those for paper files, records, or any other academic and/or employment-related material.
- 21.3 Those who handle electronic records of any kind must protect them from unauthorized modification, disclosure, and destruction to preserve the original integrity of the records.
- 21.4 Information, including data and software, is to be protected regardless of the form or medium that carries the information.

22. Intellectual Property

Because technology gives individuals the ability to access and copy information from remote sources, users must be aware of ownership rights and laws concerning intellectual property. The use of CNM's resources and systems in sending e-mail, creating and maintaining websites, installing software, downloading from the Internet, or uploading to CNM's systems and networks is contingent upon the user agreeing not to violate any of the laws and regulations.

- 22.1 The owner of a copyrighted work owns the rights to reproduction, modification, distribution, public performance and public display of these works. Many of the laws that protect the software and the works that are accessible through the internet are extremely broad.

For instance, copyright law protects "original works of authorship fixed in any tangible medium of expression. Works of authorship include the following categories: (1) literary works; (2) musical works, including any accompanying words; (3) dramatic works, including any accompanying music; (4) pantomimes and choreographic works; (5) pictorial, graphic, and sculptural works; (6) motion pictures and other audiovisual works; (7) sound recordings; and (8) architectural works." 17 U.S.C. § 102.

The Internet has provided easy methods of copying some works which are protected by the above mentioned laws. For example, peer-to-peer systems have made it extremely easy for users to share files, including music, movies and software. Furthermore, duplicating hardware has made it extremely easy to copy software without purchasing a license to use that software. In many cases, copying these files and software are acts of infringement of someone else's rights and can be legally prosecuted and/or addressed through CNM disciplinary process.

- 22.2 The punishment for violation of the copyright laws are very clear and very strict. Anyone who infringes the copyright of another may be liable for a civil penalty which

could be as much as \$30,000 for each act of infringement. As an example, if a user illegally downloads musical songs from the internet (e.g. by using a peer-to-peer system) may be held liable for \$30,000 for every illegally downloaded song.

- 22.3 User's of CNM's Information Technology resources agree not to use these resources in any way that violates federal, state, local or international law or the rights of others. User may not violate trade secret, copyright, trademark or patent rights. In appropriate circumstances, termination of accounts will be the consequence of repeat copyright infringement.
- 22.4 There are some exceptions to these laws, such as the fair use limitation described in 17 U.S.C. § 107 of the Copyright Act. This limitation is narrow and applies only in certain circumstances such as copying for news reporting, some teaching and research applications, scholarship or nonprofit educational purposes. For further clarification on the exceptions please refer to the full text of 107:Limitations on exclusive rights: Fair use.
- 22.5 Notification of potential copyright infringement using CNM's resources and systems should be reported to CNM's Information Technology Audit & Security Officer. Contact may be made through the CIT Support Center at (505) 224-4357.

23. Inappropriate Material

The intent of the College is to provide an environment that discourages harassment. Each user is responsible for using common sense and good judgment when accessing material via the Internet. Users who access materials that are considered offensive and/or obscene may be subject to disciplinary action in compliance with the Information Technology Use Policy and Administrative Directive, and/or the Sexual Harassment Policy and Administrative Directive and/or The CNM Student Code of Conduct.

CNM cannot protect individuals against the existence or receipt of material that may be offensive to them.

Offensive Material

- 23.1 If online material is visible or audible to others and there is a complaint that it is offensive or considered harassing, the offending user is expected to cooperate in resolving the complaint. This may involve turning off the offensive material or moving to a more private location. A refusal to cooperate is considered a violation of the Information Technology Use Policy, subject to disciplinary action.

Obscene Material

- 23.2 Works lacking in literary or artistic value while depicting sexual acts in an offensive way and appealing to prurient interests are considered obscene. Users should be aware

that obscene material that is visible or audible to others on campus is a violation of the Information Technology Use Policy and Administrative Directive and may be reported as a violation, subject to disciplinary action.

- 23.3 Pornography is a severe violation of the Information Technology Use Policy and, in some cases, may be a violation of federal, state and local law, subject to disciplinary and legal action.

Information Technology Use Controls

- 24. Reporting a Violation
- 25. Enforcing this Directive
- 26. Information Technology Use Violations
- 27. 3-Step Response to a Violation

24. Reporting a Violation

The reporting of Information Technology Use violations is the responsibility of every employee and student at CNM. This includes full and part-time employees, all employees who direct the work of one or more individuals, and employees who are in charge of computer labs or other areas containing Information Technology resources and systems.

25. Enforcing this Directive

Enforcing this administrative directive begins with recognizing what constitutes a violation and then strategizing and responding to the violation. A 3-Step response to a violation process has been defined and should be used as a tool when a violation occurs.

- 25.1 The Human Resources Department and the Office of the Dean of Students conduct any necessary investigations for suspected Information Technology use violations. The system administrator, department supervisors/instructors, CIT, and Campus Security serve as consultants in support of investigations.

26. Information Technology Use Violations

To maintain the integrity of CNM's Information Technology resources and systems it is necessary to identify common violations that can be addressed quickly to maintain effective technology use at CNM. Common violations are noted in the violation matrix and are identified as minor or major. This list is not intended to be all-inclusive but represents the types of offenses that are considered violations under this administrative directive. Category 1 violations are considered minor and Category 2 or 3 violations are identified as major offenses.

These violations apply to any device, whether College owned or personal, used to access CNM's systems and networks.

Engaging in activities that violate this, or other administrative directives, may result in loss of access privileges as well as possible disciplinary action.

Violation Categories

26.1 Category 1 - Minor Violation

A Category 1 (minor offense) is considered a low level offense involving non-threatening action that is offensive or disruptive. Low level offenses can also involve abuse or misuse of CNM technology systems or networks. Minor offenses include such things as drinking or eating in lab settings, or viewing images that may be offensive to another person in the area but are not illegal.

26.1.1 All minor violations should be addressed using the 3-Step Response to a Violation process. Every attempt should be made to resolve minor violations satisfactorily using the lowest level of response possible.

26.1.2 Refer to applicable area directives and College policies and procedures to resolve and explain the violation to the suspected violator.

26.1.3 Any employee who is uncomfortable attempting to resolve a violation should contact an immediate supervisor. In the case of obvious threats to CNM systems and/or networks, contact the CIT Support Center. If a situation poses any danger or threat for individuals, immediately contact Campus Security.

26.1.4 Notification and documentation of minor violations are done according to area directives. Any escalation of minor violations to major violations must follow the documentation and notification requirements of a major violation.

26.1.5 Repeated minor violations by an individual can be escalated to a major violation if the user refuses to comply with requests to discontinue the behavior.

26.2 Category 2 and Category 3 – Major Violations

A Category 2 (major offense) involves suspected violations of international, federal, state, or local law, a system/network performance threat caused by *reckless* activity, or individuals who do not comply with requests to discontinue unacceptable activities identified as Category 1 (minor) violations. This can include individuals who become physically or verbally abusive in response to a request to discontinue minor violations.

A Category 3 (major offense) involves *obvious* violations of federal, state, or local law or a system/network performance threat caused by intentional activity.

In most cases it may be difficult to determine whether a violation is a Category 2 or a Category 3 until the investigation is complete. Although they may appear the same,

intentional activity that violates Information Technology Use policy (Category 3) can result in more severe disciplinary action than reckless activity (Category 2 violation).

- 26.2.1 All Category 2 and Category 3 (major) violations should be addressed using the 3-Step Response to a Violation process.
- 26.2.2 Any emergency situation that involves risk to an individual and/or property may dictate that the normal protocol is temporarily circumvented until a threatening situation is controlled. Campus Security is involved in major violations when there is a potential risk to students, personnel or the general public, or for other pertinent reasons that require Security's involvement.
- 26.2.3 Major violations require the immediate notification of the next level of supervision in the normal reporting protocol structure. Suspicion of violations that can cause significant harm to individuals, or CNM's systems and networks, should be escalated immediately to the Human Resources Department or the Office of the Dean of Students. The CIT Support Center should also be contacted in case CIT needs to take immediate action to preserve operations. After hours, a recording refers callers to another number for assistance.
- 26.2.4 Any inappropriate behavior resulting in students being temporarily removed from facilities must be reported immediately to the next level of supervision and the Office of the Dean of Students. Inappropriate behavior resulting in employees being temporarily removed from facilities must be reported to the next level of supervision and the Human Resources Department.
- 26.2.5 Category 2 and 3 Violations require completion of the Information Technology Use Violation Report. The report and any other support documentation or physical evidence must be submitted to the Human Resources Department or the Office of the Dean of Students.

Employee violations are submitted to the Human Resources Department and student violations are submitted to the Office of the Dean of Students.

Violations involving individuals from the general public are referred to the Office of the Dean of Students. The Human Resources Department and the Office of the Dean of Students acknowledge receiving Information Technology Use Violation Reports via email response to the submitting individual or area.

- 26.2.6 The Human Resources Department or the Office of the Dean of Students conduct investigations regarding suspected Information Technology use violations. They determine if outside agencies need to be contacted.
- 26.2.7 All documentation and evidence gathered during an investigation is maintained by the office completing the investigation (the Human Resources Department or the Office of the Dean of Students) for a period of not less than 10 years. The

document files are destroyed by the Records Retention Department when the retention requirements have been met.

27. 3-Step Response to a Violation

The 3-Step Response to a Violation process is designed to assist CNM employees in responding to an Information Technology use violation. Step 1, Recognize, recommends identification and evaluation of what is actually happening. Step 2, Strategize, involves developing a plan for an appropriate response to the violation. Step 3, Respond, is based upon the category of the violation. Refer to the 3-Step Response to a Violation chart for clarification.

Definitions

28. Definitions

Access	Permission to use a technology resource according to appropriate limitations, controls, and standards.
Administrative Directive	Guiding principles, goals and processes established for College-wide use that influence and/or determine decisions and actions in compliance with Governing Board Policy
Area Directives	Guiding principles, goals and processes established within specified work areas that influence and/or determine decisions and actions in compliance with Governing Board Policy and Administrative Directives.
Authorized User	Any individual, whether student, faculty, staff, or individual external to CNM, who has been granted access privileges to specific Information Technology resources.
Category 1 Violation	A low level offense involving non-threatening action that is offensive or disruptive. Low level offenses can also involve abuse or misuse of the CNM technology systems or networks.
Category 2 Violation	A violation of federal, state, or local law, or a system/network performance threat caused by reckless activity, or repeated Category 1 violations by an individual who do not comply with requests to discontinue their behavior.
Category 3 Violation	An obvious violations of federal, state, or local law or a system/network performance threat caused by intentional activity.

Confidential Information or Data	Personal and personally identifiable information, (e.g., addresses, social security numbers, medical information) and other information as defined by the <u>New Mexico State Confidential Materials Act</u> .
Data	A representation of information in an organized manner that is stored, communicated, interpreted, or processed by automated means.
Electronic Data	Data stored in a format that can be accessed, stored, and/or manipulated electronically.
Eligible Individuals	This group includes registered students, regular and temporary faculty and staff, casual employees, and any individuals or entities approved by the CNM Administrative Vice President.
Employee Handbook	The document that contains Governing Board Policy regarding the guiding principles, goals and processes in use at CNM.
Enterprise Resources	Information Technology services that provide critical operations to CNM. These services include, but are not limited to: <ul style="list-style-type: none"> • Administrative Applications • Cable Infrastructure • Network Services/Equipment • Telephone Services/Equipment • Remote Access Services/Equipment/and Applications • Web Services/Applications/Equipment • Wireless Services/Applications/Equipment
Information Technology	The technology involved in developing, maintaining, and using computer systems, software, and networks for the processing and distribution of data.
Intellectual Property	Original works of authorship fixed in any medium of expression. A work is fixed when made sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration. Motion media, text material, music, lyrics, music video, illustrations, photographs, trademarks, slogans, and patents are examples of intellectual property.
Institutional Data	Data stored on CNM's systems and networks and/or generated by CNM employees while conducting College business.

Locked Account	An account that has been rendered inaccessible to the account owner. All files/data associated with the account remain intact and unchanged. An account may be locked by the System Administrator for a number of reasons including, but not limited to, account inactivity for a predetermined period of time, an ongoing security investigation, a violation of the Technology Use Policy, termination of employment, or discontinued association with the College. An account can be unlocked by the System Administrator when deemed appropriate.
Monitor	(1) To check systematically or scrutinize for the purpose of collecting specified categories of data; (2) a device for recording or controlling a process or activity.
Obscene Material	<p>Works lacking in literary or artistic value depicting sexual acts in an offensive way appealing to prurient interests. Factors generally used to determine the obscene nature of materials are:</p> <ul style="list-style-type: none"> • Would the average person, applying local contemporary community standards, find that the material taken as a whole, appeals to prurient interest? • Would the average person, applying local contemporary community standards, find that the material depicts or describes in a patently offensive way, sexual conduct specifically defined in applicable state law? • Would a reasonable person find that the material, taken as a whole, lacks serious literary, artistic, political, or scientific value? • Does the material describe or depict violence or simulated violence such as but not limited to murder, rape, torture, sadomasochistic abuse, or beatings in association or in conjunction with sexual conduct?
Offensive Material	Text, images or other material that may be intimidating, hostile or harassing in nature or interpretation.
Password	A combination of letters, numbers and/or symbols used to verify a person's access privileges to an Information Technology resource.
PIN	Personal Identification Number
Public Record	Any document, paper, letter, book, map, tape, photograph, recording or other material, regardless of physical form or characteristics, that is used, created, received, maintained or held by or on behalf of any public body and relates to public business,

whether or not the record is required by law to be created or maintained.

Student Code of Conduct	The document that defines the behavioral expectations of students. It contains the student discipline processes and procedures to be followed if a student violates the established Code of Conduct.
Student Handbook	The official CNM publication in which the Student Code of Conduct and other policies/guidelines related to student behavior are published. All students should keep a current copy of this publication to serve as a reference regarding behavioral issues or questions.
System Administrator	The individual responsible for the administration of resources on a system which includes: (1) access privileges; (2) physical resources; (3) installation and service/upgrades of software and hardware; (4) configuration of software and hardware; (5) securing software and data; (6) ensuring the performance and capacity of a system.
The Source	The centralized source of CNM Governing Board Policy, administrative directives and procedures that determine College-wide standard practices regarding principles, goals and processes.
User	Any individual, whether student, faculty, staff, or individual external to CNM, who uses CNM Information Technology resources.

PRIVACY RESOURCES

1. *Protocol Intrinsic to Computing Technology*

- 1.1 By virtue of having a CNM network account, (whether e-mail, web, or both), the user grants specific permission to CNM, and CNM reserves the right, to access all information stored on its systems. Accounts are not granted without this permission and are locked if such permission is withdrawn by the user.
- 1.2 Network components automatically log a variety of information, whenever any activity occurs, which includes, but is not limited to the following:
 - the Internet Protocol (IP) address of the requestor
 - date and time of the request
 - the file requested
 - the referring page (if available)
 - the type of browser used (if available)
- 1.3 Similar information is logged for telephone activity.
- 1.4 Monitoring transmissions or transactional information is necessary to ensure the security, performance, and stability of CNM's systems and networks. System administrators and other authorized personnel make every reasonable effort not to view the contents of transmissions, data, and files that are not essential to the performance of their jobs.
- 1.5 The deletion of electronically stored data on local drives by users is not necessarily permanent due to the fact that some software utility programs can retrieve deleted information from hard drives. In addition, deleted information could still reside on back-ups used to restore systems when service disruptions occur. The retrieval of data will not occur without reasonable justification.
- 1.6 Despite reasonable efforts made by CNM to secure electronic data stored and transmitted using its systems and networks, the College cannot guarantee the security of such data against unauthorized access by other users, within or outside the CNM community (e.g., harvesting of accounts by hackers, or users leaving electronic devices logged onto CNM systems and networks unattended).

2. Standard Practices

- 2.1 In general, confidential information or data pertaining to employees are not to be disclosed to third parties without the employee's written permission.
- 2.2 In general, information pertaining to student records is not to be disclosed to third parties without the student's written permission.
- 2.3 Anyone receiving a request for public information from an individual or entity outside CNM should refer the requestor to the Office of the Vice President for Administrative Services.
- 2.4 Since CNM is a public institution, electronic records and data pertaining to its administrative business are considered to be the property of CNM and/or public record.
- 2.5 It is permissible for supervisory staff to access an employee's work-related electronic files when the employee is away from work, if necessary, or if deemed reasonable, with approval from the Human Resources Department.
- 2.6 Users of CNM's Information Technology resources share the responsibility for keeping their own and the College's data private and secure by not sharing their passwords and PINs.
 - 2.6.1 Users are advised to educate themselves on the risks to their privacy when using Internet resources. To learn more about online privacy, check the following links:

Privacy in Cyberspace Rules of the Road for the Information Superhighway

(<http://www.privacyrights.org/fs/fs18-cyb.htm>)

EFF's (Electronic Frontier Foundation) Top 12 Ways to Protect Your Online Privacy (http://www.eff.org/Privacy/eff_privacy_top_12.html)

CDT's (The Center for Democracy and Technology) Guide to Online Privacy (<http://www.cdt.org/privacy/guide/basic/topten.html>)

Federal Trade Commission: Privacy Initiatives

(<http://www.ftc.gov/privacy>)

Employee Monitoring: Is There Privacy in the Workplace?

(<http://www.privacyrights.org/fs/fs7-work.htm>)

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (<http://www.cybercrime.gov/s&smanual2002.htm>)