NORTHERN NEW MEXICO COLLEGE

Information Technology

Department

Policies and Procedures Manual

Contents

LONG DISTANCE TELEPHONE CALLS 5
1. General 5
2. Authorization to Place Long Distance Calls at College Expense 5
2.1. Security 5
2.2. Deactivation 5
3. Reimbursement for College Business Long Distance Calls 5
ACCEPTABLE COMPUTER USE 6
1. General 6
1.1. Departmental Computer Use Policies and Procedures 6
1.2. Computing Services 6
2. Rights and Responsibilities 7
2.1. User Responsibilities 7
2.1.1. Copyrights and Software Licenses 7
2.1.3. Software Developed Internally 8
2.1.4. Computer Security 8
2.1.5. Computer Accounts and Passwords 8
2.1.5.1. Account Authentication 8
2.1.5.2 Account Termination and Locking 9
2.1.6. Computer and Data Security 9
2.1.6.1. Physical Security 9
2.1.6.2. Information Security 9
2.1.7. Computer Viruses and Anti-virus Software 9
3. Unacceptable Computer Use 9
3.1. Security Violations Users shall not 9
3.2. Legal Violations 10
3.3. Other Misuse 10
4. Incidental Personal Use 11
5. Privacy Limitations 11
6. Reporting Procedures 12
7. Sanctions 12
COMPUTER SECURITY CONTROLS AND ACCESS TO SENSITIVE AND PROTECTED INFORMATION 13

1. General 13
2. Access to Departmental Systems 13
3. Access to Computer Systems Containing Sensitive and Protected Information 14
3.1. Remote Access 14
3.1.1. Approval for Remote Access 14
3.1.2. Sensitive Data 15
4. System Protection 15
4.1. Virus Protection 15
4.2. Privacy and Confidentiality 15
4.3. System Integrity 15
4.4. Data Loss Protection 15
4.5. Records Management 15
5. Security Violation Handling 16
6. User Responsibility and Accountability 16
7. Sanctions 16
Text Messaging Notification Policy 16
1. General 16
2. Emergencies 17
2.1 Scope 17
2.2 When is it appropriate? 17
2.3 Approvers 17
2.4 Target Groups 18
2.5.1 Sender 18
2.5.2 Subject 18
2.5.3 Where to get more information 18
3. Work-related Incidents 18
3.1 Scope 18
3.2 When is it appropriate? 18
3.3 Approvers 19
3.4 Recipients 19
3.5 Format of message 19
4. Further Advice 19
STUDENT EMAIL 19

1. General 19
2. Student Responsibilities Students are responsible for: 19
INFORMATION SECURITY 20
1. General 20
2. Northern Information Security Program 20
2.1. Protected Information 21
2.2. Information Security Plan Coordinator 21
2.3. Risk Assessment 21
2.4. Employee Management and Training 22
2.6. Departmental Responsibilities 22
2.7. College-Wide Responsibilities 22
3. Compliance by Service Providers 22
4. Monitoring and Testing 22
5. Evaluation and Adjustment 23
INFORMATION TECHNOLOGY (IT) GOVERNANCE 23
1. General 23
1.1. Information Technology Governed by this Policy 23
2. Roles and Responsibilities 23
2.1. Northern IT Director 23
3. Overview of IT Policies, Standards, Guidelines, Processes, and Procedures 23
4. Northern IT Policies 24
4.1. Development 24
4.2. Approval and Communication 24
4.3. Compliance 25
5. IT Standards 25
5.1. Development 25
5.2. Approval and Communication 25
5.3. Compliance 25
6. IT Guidelines 26
6.1. Development 26
6.2. Approval and Communication 26
6.3. Compliance 26
7. IT Processes and Procedures 26

7.1. Development.....26
7.2 Approval and Communication.....26
7.3. Compliance.....26
7.4. Review and Revision.....26
8. Policies Establishment.....26

LONG DISTANCE TELEPHONE CALLS

1. General

Only long distance calls for official Northern business should be charged to the College. Charging long distance telephone calls for personal or other non-College purposes is prohibited and constitutes misuse of College funds. Personal calls made from College telephones must be charged to the caller's home telephone or personal credit card, to the called party, or to another non College source. If an emergency situation requires an employee to charge a personal long distance call to the College, the employee must reimburse the College. Since the call is charged to the department, reimbursement is made to the department's account.

2. Authorization to Place Long Distance Calls at College Expense

Each individual who is authorized by a department to place long distance calls for College business will be issued an individual authorization code which can be used to place calls from College phones. Calling cards are issued to individuals who place long distance calls for College business from non-College phones. Authorization codes and calling cards are issued to individuals by the College Information Technologies. Long distance charges are billed to the account specified by the requesting department. Information Technologies provides departments with invoices itemized by authorization code and calling card numbers which enable a department to monitor long distance calls. Departments should maintain long distance telephone logs to ensure the accuracy and appropriateness of College long distance charges and reconcile the logs to the invoices provided by Information Technologies. Charges billed to an account in error should be reported to Information Technologies.

2.1. Security

Individuals assigned long distance authorization codes and calling cards are responsible for ensuring the security of the codes and cards, and should not disclose or share them with others. Individuals should report compromised authorization codes or lost calling cards to Information Technologies immediately.

2.2. Deactivation

When an individual transfers to another department, his/her authorization code and/or calling card is deleted and a new authorization code and/or calling card is issued and charged to the new department. Upon separation from the College, the employee must return all calling cards to the Information Technologies Department. The department requesting authorization codes and calling cards is responsible for notifying Information Technologies of an employee's change of status and requesting that authorization codes and/or calling cards be deactivated. Any charges incurred by the continued use of an authorization code or calling card due to a department's failure to request that they be deleted or changed will be billed to the responsible department's account.

3. Reimbursement for College Business Long Distance Calls

Long distance calls made for College business purposes using an employee's personal telephone services (including a personal calling card, cell phone, or home phone line) may be reimbursed. The employee must attach a copy of the telephone invoice with the pertinent calls highlighted and an explanation of the expense to the applicable form.

ACCEPTABLE COMPUTER USE

1. General

As an institution of higher learning, Northern New Mexico College encourages, supports, and protects freedom of expression as well as an open environment to pursue scholarly inquiry and to share information. Access to information technology, in general, and to the Internet, in particular, supports the academic community by providing a link to electronic information in a variety of formats and covering all academic disciplines. The computing and network resources, services, and facilities of the College are limited and should be used wisely and carefully with consideration for the needs of others. As with any resource, there is a possibility of misuse. In an attempt to prevent or mitigate such misuse, this policy outlines proper and improper behaviors, defines misuse and incidental use, explains rights and responsibilities, and briefly reviews the repercussions of violating these codes of conduct.

Northern New Mexico College provides computing services to College faculty, staff, and students. These services are intended primarily for furthering the education, research, and public service mission of the College and may not be used for commercial purposes or profit-making. This Policy is applicable to all individuals using College-owned or -controlled computer equipment, communications equipment, data - network (wired and wireless), storage devices, and computer-related facilities, whether such persons are students, staff, or faculty. All College policies including, but not limited to, intellectual property protection, privacy, misuse of College equipment, sexual harassment, hostile work environment, data security, and confidentiality shall apply to the use of computing services.

1.1. Departmental Computer Use Policies and Procedures

Individual departments within the College may define “conditions of use” for information resources under their control. These statements must be consistent with this overall policy but may provide additional detail, guidelines, and/or restrictions. Such policies may not relax, or subtract from, this policy. Where such “conditions of use” exist, the enforcement mechanisms defined within these departmental statements shall apply. Individual departments are responsible for publicizing both the regulations they establish and their policies concerning the authorized and appropriate use of the equipment for which they are responsible. In such cases, the department administrator shall provide the cognizant vice president and the College Director of IT with a copy of such supplementary policies prior to their implementation. Where the use of external networks is involved, policies governing such use also are applicable and must be adhered to.

1.2. Computing Services

For the purposes of this policy computing services include the following:

- All College data, information, and information systems (including computer applications used by the College that are hosted elsewhere),
- All College computer hardware, software, multi-media, and communication services including all computer resources, communications equipment, and data networks— wired and wireless,
- All College telephones, mobile phones, smart phones, storage devices, and personal digital assistants, and

- All digital assets owned, managed or leased by the College and any that may be entrusted to the College by other organizations (e.g. cloud computing services as well as any other future computing device, service, system, or application.)

2. Rights and Responsibilities

The use of College computing services is a privilege. Users who have been granted this privilege must use the services in an appropriate, ethical, and lawful manner. Unauthorized access is prohibited and may be monitored and reported to the proper authorities. The College does not provide a warranty, either expressly or implied, for the computing services provided. The College reserves the right to limit a computer user's session if there are insufficient resources, and to cancel, restart, log, record, review or hold a job, process, network connection or program to protect or improve system or network performance if necessary.

The College network is large and complex and supports mission critical functions such as patient care, payroll, academic classes, Internet access, and electronic mail.

2.1. User Responsibilities

Users are responsible for all their activities using computing services and shall respect the intended use of such services. Whenever a computing facility has specific rules and regulations that govern the use of equipment at that site and users shall comply with those rules and regulations governing the use of such computing facilities and equipment in addition to any over-arching College policies such as this one. Users must understand and keep up-to-date with this policy and other applicable College computer policies and procedures.

Users shall respect all copyrights including software copyrights. Users shall not reproduce copyrighted work without the owner's permission. In accordance with copyright laws, including the Digital Millennium Copyright Act, college's legal counsel, upon receipt of official notice from a copyright owner, may authorize blocking access to information alleged to be in violation of another's copyright. If after an investigation information is determined by college's legal counsel to be in violation of another's copyright, such information will be deleted from College computing systems.

2.1.1. Copyrights and Software Licenses

Users of College computing resources must comply with copyright law and the terms of licensing agreements, including software licenses, before accessing or using copyrighted material on the Internet. Users are responsible for determining what licenses or permissions are necessary and for obtaining such permissions or licenses before using College computing resources. Purchased music, movies, software, and other multi-media files usually include a license that gives you permission to make copies, change formats or to share the file with others.

Generally, software which the College is not permitted or not licensed to use shall not be installed on College computing services; however, software which has been personally acquired is permitted to be installed on College computing services so long as the user who has installed the software is able to prove s/he is legally permitted to do so (this is usually done by retaining and providing the license upon request.)

File-sharing applications often involve the unlawful copying or distribution of copyrighted material without permission or license from the copyright owner. Anyone who sends or receives files using file-sharing software may be engaging in an unlawful act unless (a) the user is the copyright owner or has permission from the copyright owner, (b) the material is in the public domain, or (c) fair use or another exception to copyright law applies.

Upon receipt of information alleging that a user may be engaged in unauthorized file sharing of copyrighted material or is in violation of licensing obligations or other copyright law, the College may, without notice, immediately suspend, block or restrict access to an account. The College may take such action when it appears necessary in order to protect the security or integrity of computing resources, or to protect the College from liability.

Users who violate copyright law or license terms may be denied access to College computing resources, and may be subject to other sanctions and disciplinary actions, including but not limited to expulsion or discharge from the College.

In accordance with its legal obligations, the College will continue to develop plans to combat the unauthorized use and distribution of copyrighted materials, including the possible use of technological deterrents. The College will also continue to provide information on alternatives to illegal file-sharing.

2.1.3. Software Developed Internally

College personnel may develop computer programs using College computing resources. Such software may be subject to the College's Intellectual Property Policy.

2.1.4. Computer Security

Individuals using computing services are responsible for keeping accounts and passwords confidential and for safeguarding all College data and information, especially those covered by state and federal regulations such as FERPA, regardless if it is being stored on College computing resources, stored on non-college resources, or being transmitted over communication networks.

2.1.5. Computer Accounts and Passwords

The College, through IT and departments, provides computer accounts to authorized users for access to various College systems. These accounts are a means of operator identification and passwords are used as a security measure. An individual's computer account shall not be shared. Account use is a privilege, not a right.

2.1.5.1. Account Authentication

Passwords, PINs, and other identifiers authenticate the user's identity and match the user to the privileges granted on College computers, computer networks, systems and computing resources. A password is a security measure designed to prevent unauthorized persons from logging on with another person's computer account and reading or changing data accessible to that user. Users should create passwords carefully and handle them with care and attention. For this security feature to be effective, the user must protect the secrecy of his/her password. Each user should:

- choose a password that is s minimum of eight characters to include a number, capital letter, and special character
- change his/her password at a minimum of every ninety (90
- days and at any time the user believes the password may have been compromised,

avoid writing the password down, and not disclose or share the password with anyone.
- Similar measures apply to all authentication methods such as PINs.

2.1.5.2 Account Termination and Locking

When an individual leaves the College, his or her account(s) must be locked as soon as reasonably possible and, subsequently, deleted within a reasonable time. If misuse or theft is detected or suspected, account(s) will be locked according to the College's procedures.

2.1.6. Computer and Data Security

Everyone at the College shares responsibility for the security of computer equipment, data, information and computing resources.

2.1.6.1. Physical Security

Everyone is responsible for the proper use and protection of College computer resources. Examples of protection measures include:

- locking areas after business hours or at other times when not in use;
- taking special precautions for high-value, portable equipment;
- locking up documents and computing resources when not in use; and

2.1.6.2. Information Security

Security of data and information is an essential responsibility of computer system managers and users alike. For example, users are responsible for:

- ensuring the routine backup of their files;
- using data only for approved College purposes; and
- ensuring the security and validity of information transferred from College systems.

2.1.7. Computer Viruses and Anti-virus Software

All College departments, though department heads or designees, shall ensure anti-virus software is installed on College computing resources when technically possible and that the software is active and kept up to date. This requirement applies to all computer servers as well as all desktop and laptop computers. This will help ensure that College computing services and digital assets are not compromised, misused, deleted or destroyed.

3. Unacceptable Computer Use

The College reserves the right to block access to any external electronic resources that are deemed in violation of this Policy. If it is determined, after an investigation by the appropriate office, that the user violated federal or state law, rules or regulations or College policy by misusing College computing services. The College will disclose illegal or unauthorized activities to appropriate College personnel and/or law enforcement agencies.

3.1. Security Violations Users shall not

- attempt to defeat or circumvent any security measures, controls, accounts, or record-keeping systems;

- use computing services to gain unauthorized access to Northern's or anyone else's computing services;
- intentionally alter, misappropriate, dismantle, disfigure, disable or destroy any computing information and/or services;
- knowingly distribute malware (i.e. computer viruses, worms, Trojans, or other rogue programs).

3.2. Legal Violations

Users shall not use computing services:

- for unlawful purposes, including fraudulent, threatening, defamatory, harassing, or obscene communications;
- to invade the privacy rights of anyone;
- to disclose student records in violation of FERPA;
- to access other computing services (i.e. other Northern computers or computer systems for unauthorized purposes;
- to access or disclose financial information in violation of the Gramm-LeachBliley Act or the College's Information Security Program;
- to access or disclose any non-public or personally identifiable information about a patient, employee, or student without having a legitimate College purpose
- to violate College policy, state law, or federal law, including but not limited to copyright laws.

3.3. Other Misuse

Users shall not use computing services:

- in violation of any College contractual obligation, including limitations defined in software and other licensing agreements;
- in a way that suggests College endorsement of any commercial product (unless a legal agreement exists and any communication or computing activity has been pre-approved by an appropriate vice president);
- to conceal one's identity when using computing services, except when the option of anonymous access is explicitly authorized,
- to possess or distribute obscene or pornographic material unrelated to College instruction, research, or business needs (students are excluded from this provision);
- to masquerade or impersonate another,
- by physically or electrically attaching any device to a College computer, communications devices, or network connection that negatively impacts the performance of any other College computing service;
- to send chain letters, pyramid schemes or unauthorized mass mailings;
- to send non-work or non-class related information to an individual who requests the information not be sent, or
- to send commercial or personal advertisements, solicitations, or promotions.

Users should understand that, due to their nature, electronic communications can be intentionally or unintentionally viewed by others or forwarded to others, and are therefore inherently not private. In addition, addressing errors, system malfunctions, and system management may result in communications being viewed and/or read by other individuals and/or system administrators.

In electronic communications, users must state whether they are speaking for themselves or in an official capacity for the College. Electronic communications that represent the College sent to non-Northern addresses must be done in a professional manner.

4. Incidental Personal Use

The College allows incidental personal use of computing services. Such use must not interfere with an employee fulfilling his or her job responsibilities, consume significant time or resources, interfere with other users' access to resources, be excessive as determined by management, or otherwise violated any federal or state laws, any individual college or departmental policies or codes of conduct, or College policies. Each department should document and communicate what use is acceptable.

5. Privacy Limitations

Users of College computing services, including managers, supervisors, and systems administrators shall respect and protect the privacy of others, in accordance with all applicable state and federal laws, regulations and College policies. Although the College is committed to protect individual and information privacy, the College cannot guarantee the security or privacy of correspondence and information stored and transmitted through College computer networks and systems. Since confidential information is often stored on desktop machines, displayed on screens, or printed on paper that could be in public view, users need to control access by:

- using passwords;
- turning screens away from public view;
- logging out of systems when leaving the work area;
- shredding reports containing private information prior to disposal; and
- clearing confidential information off desks in public areas.

While the College does not routinely monitor individual usage of its computing services, the normal operation and maintenance of the College's computing services require the backup and storage of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendering of services. Similarly, the College does not, in the regular course of business, monitor the content of computing services on its various networks. However, suspicious aggregate behavior, official requests from authorities, forensic evaluation or discovery for purposes of civil litigation, or indications of a security incident, for example, can cause network activities or computing services to be reviewed. It is the right of the College to monitor and review any activities on its resources. It is best, therefore, to assume that any and all actions taken or activities performed using College computing services are not private.

The College may also access and examine the account (e.g. any and all computer accounts on any College computing resource, e-mail boxes, file shares, local or networked storage) of an individual user under the following circumstances and conditions:

- if necessary to comply with federal or state law, or
- if there is reasonable suspicion that a law or College policy has been violated and the examination of the account is needed to investigate the apparent violation, or
- as part of an investigation involving an administrative claim or charge, arbitration or litigation, or if required to preserve public health and safety.

Requests for access based on reasonable suspicion must be approved in writing, in advance, by the cognizant vice president. If access to a faculty member's account is being requested, the President of the Faculty Senate must be notified in conjunction with the request for approval. Each request must specify the purpose of access and such access will be limited to information related to the purpose for which access was granted. If such access is being requested by a vice president, access must be approved by the President. If such access is being requested by the President, access must be approved by the Northern Board of Regents. The Regents' Internal

Auditing Policy authorizes the College Audit Department full and unrestricted access to all College records, including but not limited to those contained in computer files, discs, and hard drives.

Accessing an employee's computer files for work-related, non-investigatory purposes (i.e., to retrieve a file or document needed while the employee who maintains the file or document is away from the office) is permitted and does not require authorization by a vice president as long as access is limited to the work-related need. When an employee separates from the College, work-related files, including but not limited to research data, as well as all records made or kept in any College electronic medium, remain the property of the College.

Communications and other documents made or kept by means of College computing services are generally subject to New Mexico's Inspection of Public Records Act to the same extent as they would be if made on paper. Therefore, all employees are urged to use the same discretion and good judgment in creating electronic documents as they would use in creating written paper documents.

6. Reporting Procedures

Suspected violations of this policy (e.g. any incidents involving the unauthorized access to, destruction of, or misuse of computing services by employees, faculty or students) must be brought to the attention of the dean, director, or department head, and the College IT Security Office. In the case of a criminal violation, the IT Office will notify Campus Security. Violations by non-employees will be referred to the appropriate authorities.

7. Sanctions

The misuse, unauthorized access to, or destruction of College computing services in violation of applicable laws or College policy may result in sanctions, including but not limited to withdrawal of use privilege; disciplinary action up to and including, expulsion from the College or discharge from a position; and legal prosecution.

COMPUTER SECURITY CONTROLS AND ACCESS TO SENSITIVE AND PROTECTED INFORMATION

1. General

Management of College computing services must ensure the rights and responsibilities provided for in Policy 2500 while also ensuring system and data availability, reliability, and integrity. Therefore, all departments operating College owned computers, including those operated by faculty, staff, and students, must develop departmental security practices which comply with the security practices listed herein. In addition, departments must have environment-specific management practices for business functions such as maintenance, change control procedures capacity planning, software licensing and copyright protection, training, documentation, power, and records management for computing systems under their control. This may be done by hiring a qualified employee, sharing resources with other departments, or contracting with College Information Technologies (IT). IT is available to assist and advise departments in planning how they can carry out compliance with this and other computer technology-related policies.

Departments must document and periodically review established practices.

Department heads or designees are responsible for computer security awareness and for ensuring reasonable protection of all departmental computing systems within their purview against breaches of security, through methods such as virus protection, firewalls, encryption, patch management, change control, and password usage. Department heads or designees should ensure users of their systems have the necessary training for appropriate use of the system.

2. Access to Departmental Systems

Access to departmental computing systems must be authorized by the department head or designee. Access to College computing systems containing or transmitting sensitive and protected information must be authorized by the department head and approved by the College designated data custodian. To ensure confidentiality, special attention should be taken when authorizing system access to vendors and/or contractors, including those repairing and/or maintaining computers and computing devices. When possible, it is advisable to have vendors and/or contractors sign a confidentiality agreement. Computer access control also includes physical security to Northern equipment and information, such as: locks on doors/windows for equipment and storage, locking paper files, and paper shredders. The department head or designee ensures proper management of computer accounts and user identification by:

- handling system user authentication securely (e.g. passwords, PIN numbers, access codes);
- terminating an account in a timely manner when an individual's affiliation with the College is terminated or completed;
- following established policies and procedures and legal due process when violations are detected or suspected.

3. Access to Computer Systems Containing Sensitive and Protected Information

An individual who requires access to sensitive and protected information must be authorized by the data custodian responsible for the specific application. All contractors and vendors who have access to sensitive or protected information are required to sign confidentiality agreements prior to gaining such access. The data custodian is an individual officially appointed to authorize access to the system and ensure application-specific security. Authorization will only be granted to those individuals with a demonstrated need to use such information and/or electronic processes and who has taken the required training applicable to the system being requested. The data custodian will advise the individual on the system specific process used to authorize and gain access to the requested system. The data custodian or designee must review and approve each request for access to a specific system, ensure that all required training has been taken prior to granting access, and authorizes access based on the user's business need and role in accordance with application-specific access procedures. Contact IT for list of Data custodians.

3.1. Remote Access

For the purposes of this Policy, "remote access" is defined as any means by which any faculty, staff, student employee, consultant, vendor or affiliate connects to the Northern Network using a non-Northern network device or service to access sensitive or protected information. This provision applies regardless of the type of device being used or if the device is College owned or personally owned. IT, department heads, designees and users share the responsibility for ensuring appropriate security mechanisms are in place to preserve the integrity of the network, to preserve the data transmitted over that network, and to maintain the level of confidentiality of the data at all times. Because of the increased level of risk inherent with remote access, strong security measures are required. When a user accesses sensitive or protected information remotely, identification and authentication of the user shall be performed in such a manner as to not disclose the password or other authentication information that could be intercepted and used by a third party.

3.1.1. Approval for Remote Access

Users will be allowed to access to sensitive or protected information from a remote location only upon approval by the data custodian. Once approved, the user is responsible for ensuring adequate security measures are in place at the remote location for secure transmission of agency data and protection of College computing resources. IT can assist the user in identifying the appropriate protection mechanisms necessary to protect against theft of College resources, unauthorized disclosure of information, and unauthorized access to the College network. The user is responsible for ensuring devices used for remote access are protected by a firewall and virus scans, and contain all up-to-date security patches.

Northern recommends that users leave data on Northern servers as much as possible and not copy sensitive data onto any mobile computing device. Storage of sensitive data and protected information on a non-Northern computer is prohibited unless a formal written exemption is granted by the data custodian. When stored remotely on a Northern computing device the data must be encrypted.

3.1.2. Sensitive Data

Users should be especially careful with the following types of data:

- confidential financial information
- account names and passwords
- social security and/or credit card numbers
- personal contact names and phone numbers
- decryption keys or pass-phrases

4. System Protection

Department heads are responsible for protecting the systems under their control from system intrusion, compromise, or data loss.

4.1. Virus Protection

Virus detection and elimination software is essential to protect College data and systems. Department heads, or designees are responsible for maintaining the latest version of an antiviral software and current updates on their computers. Systems must have active virus protection turned on with each system scanned regularly. Assistance with virus protection and software are available from IT at.

4.2. Privacy and Confidentiality

Department heads, or designees must take appropriate measures to ensure privacy and confidentiality of system data in accordance with applicable laws and policies such as:

"Social Security Numbers" Policy 2030, UBP "Identify Theft Protection Program" Policy 2040, UBP "Information Security" Policy 2550, UBP

Family Educational Rights and Privacy Act of 1974

New Mexico Inspection of Public Records Act

4.3. System Integrity

Department heads, or designees may monitor and investigate systems or jobs under their control for appropriate use of resources, to protect or improve system performance, or in compliance with audit or legal requests. Jobs, procedures, and/or functions may be restricted or limited to ensure system integrity. Departments must maintain current versions of system software and security patches, especially when there are known security issues.

4.4. Data Loss Protection

For all computing systems that store or process sensitive or protected information department heads or designees are responsible for ensuring all data is stored on the NNMC File System. The sensitive data files are backed up shall be backed up daily and stored offsite. An acceptable retention period shall be enforced by no less than two weeks. Limited access to this sensitive data shall be enforced.

4.5. Records Management

Department heads, or designees are responsible for computerized data retention and backup procedures that comply with College Records Management requirements for classification and retention of College information.

5. Security Violation Handling

Department heads, or designees should detect and correct any non-compliance with this and other College computer policies. In addition to following any College or department mandated security incident reporting process, any and all employees, faculty, or staff who reasonably believe:

- there has been a breach to any College computer application or system, there has been a breach to Northern's computer security controls (i.e. a computer has been hacked or somehow has been compromised by an unauthorized person), or
- there has been a violation of this Policy are required to report the incident, within twenty-four (24) hours of becoming aware of the violation or breach, to the Northern IT Director or the Northern Security Office.

All investigations should follow proper investigative procedures to ensure confidentiality and due process. Any employee who detects or suspects noncompliance should report such conduct to the department head.

6. User Responsibility and Accountability

Users are responsible for proper use and protection of College information and are prohibited from sharing information with unauthorized individuals. The web-based information systems allow an authorized user the ability to complete transactions directly on-line and forward the forms to the appropriate administrators for approval. By completing a form on-line, the user accepts responsibility to follow all applicable policies and procedures.

7. Sanctions

Employees who do not demonstrate due care in the administration of their duties as required by this Policy may be subject to sanctions, including withdrawal of privilege to enter information directly into the system; and/or disciplinary action, up to and including, discharge.

Text Messaging Notification Policy

1. General

The increasing and almost universal use of mobile phones has opened up a new avenue of opportunity for communication between NNMC and its staff and students.

This policy sets out the way in which NNMC will use Short Message Service (SMS) text messaging appropriately to pass on important information to staff and students. The use of SMS messaging is intended to sit alongside other existing forms of communication such as letters, email, social networking sites (Facebook and Twitter) and the College's website. The immediate delivery of SMS messages gives it an advantage over other forms of communication: most students have their mobile phones with them all the time and the message is likely to be received much sooner.

Text messaging has wide accessibility. People who are blind or visually impaired can use mobile phones, and some mobile phones have text-to-speech capability, meaning that individuals can listen to text messages.

Data Protection and privacy issues have been taken into account in preparing this policy. In some cases, people will be asked if they wish to 'opt-in' to receive particular types of messages. In others, for example where messages are sent for administrative purposes, people will be asked if they wish to 'opt-out'. However, there may be emergency circumstances in which NNMC will need to contact as many staff and students as possible, ignoring personal preferences (which is permissible if it is in the 'vital interests of the data subject' – Data Protection Act Schedule 2(4)). Phone numbers may be stored by third parties for the purpose of sending messages, but names will not be stored. There may, very rarely, be the need to send a message for test purposes.

There are a number of scenarios in which an SMS message could be very useful, e.g.

- Emergencies:
  An outbreak amongst the student population o A fire, flood, or similar incident in a College building o Any serious crime or terrorism incidents
- Work-related incidents:
  Messages to support staff about equipment/environment failures
- Other usage:
  Lecture room changes

However, the usefulness of text messaging depends on having reliable data. The mobile numbers will be taken from data collected from staff and student databases so it is important that these phone numbers are kept up to date. This will be achieved by means of email reminders or Portal announcements to staff and students to keep their details up to date and directions for how to do so.

2. Emergencies

2.1 Scope

Messages whose content is deemed to be essential or urgent.

2.2 When is it appropriate?

Incident and crisis management is handled by a team of senior managers. The team may decide a text message is appropriate whenever it is considered important to contact a group of people urgently for reasons of health or safety.

It should be noted that there is no guarantee that text messages will be delivered promptly or at all by the mobile phone companies. In some types of emergency, e.g. a terrorist incident, the emergency services may commandeer the mobile phone network, so no messages will get through.

Simultaneous, multiple approaches are essential. Text messages must be supplemented by other means of communication, such as emails, messages issued via Facebook or Twitter or information posted on the College website, to ensure that as many of the target audience as possible receive the message.

2.3 Approvers

A request to send a message to one of the College-wide lists must be approved by the President of the College, or her designated authority to approve requests.

Authorization will be given for a message only if:

- it is considered that it is important to get the message to a significant number of the recipients as soon as possible;
- the content is both appropriate and factually correct; o the message format meets the guidelines.

2.4 Target Groups

It is possible to send messages to the following groups:

- All staff, faculty and students
- All staff and faculty
- All students

Further groupings may be added in the future.

2.5 Format of message

Messages should be no longer than 160 characters and should address the student or staff member directly, i.e. as 'you'. They should include essential points, and should avoid 'text speak', e.g. write 'you', not 'u'; and 'for', not '4'. Non-Latin alphabet characters should be avoided, as they may decrease the maximum message size to 140 or even 70 characters.

2.5.1 Sender

All messages must start with the words 'Eagle Alert:' so that the recipients of the text can see that it is an official message from the College requiring their attention.

2.5.2 Subject

The message must clearly indicate what it concerns.

2.5.3 Where to get more information

The message should indicate where more information can be sought, e.g. 'see www.nnmc.edu' if the College's website is operational, or 'check email for details'.

3. Work-related Incidents

3.1 Scope

Messages that are sent to one or more staff members relating to incidents at work. These could include, for example, alerts or work instructions relating to maintenance or equipment failures.

3.2 When is it appropriate?

A text message may be appropriate to communicate with a member of staff about matters relating to his or her job, where that person is likely to be moving around the campus, or 'on call'. It is impossible to give a definitive list of possible applications; the deciding factor has to be whether it is an effective means of communication.

3.3 Approvers

See 2.3 above

Authorization should be given for a particular message only if:

- the distribution list is appropriate, and
- the content is both appropriate and factually correct.

3.4 Recipients

Information Technology Department should ensure that the list of numbers is kept up to date and reviewed at least every semester. People issued with mobile phones by the College for work purposes may not opt-out of receiving text messages.

3.5 Format of message

- Messages should be no longer than 160 characters.
- The message must clearly indicate what it concerns.
- It should be clear who has sent the message.

4. Further Advice

Message senders need to be aware of:

- The principles of the Data Protection Act 1998 and the College's guidance relating to security measures for safeguarding personal data.

See security.nnmc.edu

STUDENT EMAIL

1. General

There is an increasing need for fast and efficient communication with currently enrolled students in order to conduct official business at the College. Each student has free access to a College network ID (NetID) and email account for use throughout the time the student is registered for classes. Accordingly, email is an available mechanism for formal communication by the College with students but is not the only official method of communication. Upon admission, students are required to obtain a Northern NetID and corresponding email account. The Northern email shall be considered an appropriate delivery method for official communication by Northern New Mexico College with students unless otherwise prohibited by law. Official communication includes, but is not limited to, academic deadline notifications, billing statements, and campus alerts. The College reserves the right to send official communications to students by email with the full expectation that students will receive email and read these emails in a timely fashion. Faculty will determine how to use electronic communication for instructional purposes, and specify their requirements in the course syllabus, which students must comply with.

2. Student Responsibilities Students are responsible for:

- checking their email frequently (at a minimum of once per week) in order to stay current with College-related communications;
- ensuring there is sufficient space in their accounts for email to be delivered; and
- recognizing that certain communications may be time-imperative.

Students will not be held responsible for a substantial interruption in their ability to access a message if system malfunctions or other system-related problems prevent timely delivery of, or access to, that message (e.g. power outages or email system viruses). Students should check their email frequently to prevent problems caused by a brief system failure.

Students who choose to have their email forwarded to a private (unofficial) email address outside the official College net ID/email address (@nnmc.edu) do so at their own risk. The College is not responsible for any difficulties that may occur with privacy or security, in the proper or timely transmission, or in accessing email forwarded to any unofficial email address. Such problems will not absolve students of their responsibility to know and comply with the content of official communications sent to students' official Northern email addresses. Failure to check email frequently or email returned to the College with "mailbox full" or "user unknown" are not considered acceptable excuses for failing to know about and comply with official email communication.

Students should report problems with College email or access to the Help Desk@ 505.747.2259 2550

INFORMATION SECURITY

1. General

The College is committed to protecting and safeguarding all data and information that it creates, collects, generates, stores, and/or shares during the generation and transmission of knowledge as well as during the general operation and administration of the College. The College is also committed to complying with all federal and state laws pertaining to securing this data and information and preventing its disclosure to unauthorized individuals. These laws include, but are not limited to, the Financial Services Modernization Act of 1999, also known as the GrammLeach-Bliley Act or GLBA. In 2003, the Federal Trade Commission (FTC) confirmed that higher education institutions are considered financial institutions under this federal law and promulgated the GLBA Safeguards Rule, 16 CFR Part 314, which requires higher education institutions to have an information security program to protect the confidentiality and integrity of personal information. This policy describes the basic components of the Northern Information Security Program which applies to employees (student, staff, and faculty), contractors, vendors, volunteers, and all other individuals who work with Northern data and information.

2. Northern Information Security Program

The Northern Information Security Program is designed to protect the confidentiality, integrity, and availability of protected information; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of protected information that could result in substantial harm to any student, parent, employee, or customer of the College. This program includes the process for identification of risks and defines responsibilities for safeguarding information, monitoring the effectiveness of the safeguards, evaluating service providers, and updating the program itself.

2.1. Protected Information

The GLBA Safeguards Rule mandates that the Northern Information Security Program be designed to safeguard non-public, personally identifiable financial information

- that is provided to the College,
- results from any transaction with the consumer or any service performed for the consumer (i.e. students, faculty, staff, employees, associates, donors, patients), or
- is otherwise obtained by the College.

The Northern Information Security Program defines what specific data elements and information (and in what context) constitute to-be-protected non-public, personally identifiable financial information, which includes but is not limited to:

- social security numbers,
- credit card number, and
- bank routing and account numbers when used in conjunction with the account owner's name.

2.2. Information Security Plan Coordinator

The College Director of Information Technology is designated as the Information Security Program Coordinator, a specific role required by the GLBA. This position is responsible for:

- developing and implementing the Northern Information Security Program;
- identification of risks to confidentiality, integrity, and availability of protected information;
- designing and implementing appropriate safeguards;
- evaluating the security program; and
- making adjustments to reflect relevant developments or circumstances that may materially affect these safeguards, including changes in operations or the results of security testing and monitoring.

2.3. Risk Assessment

The Northern Information Security Program will include processes and procedures to assess the risk to the College's information systems. Information systems include the hardware and software components of the computing infrastructure as well as individual personal computers, personal digital assistants, phones, servers, networks, and peripheral technologies used for the processing, storage, transmission, retrieval, and disposal of information. Risks to the College's information systems extend beyond computer-related hardware and software to include, for example, hiring procedures; data handling procedures; individuals who have access to information systems and the data therein; and the buildings and equipment that contain any aspect of an information system including the transmission of protected information.

2.4. Employee Management and Training

The success of the Information Security Program depends largely on the employees who implement it. The Director of Information Technology will coordinate with deans, directors, and heads of departments that have access to protected information to evaluate the effectiveness of departmental procedures and practices relating to access to and use of protected information. The Northern Information Security Program details recommended administrative safeguards designed to train personnel, increase awareness, and reduce risks to the confidentiality, integrity, and availability of protected information such as:

- mandatory information assurance training;
- periodic audits to ensure individuals have only the appropriate level of information system access rights and permissions required to perform their jobs;
- periodic reviews of job descriptions and position requirements to ensure the appropriate levels of reference and background checks are conducted before hiring decisions are made;
- non-disclosure and confidentiality statements required when appropriate; and
- periodic evaluations of each individual's understanding of college and/or departmental data handling procedures.

2.6. Departmental Responsibilities

Deans, directors, and heads of departments that have access to protected information are responsible for informing employees of ongoing updates to security measures, ensuring employees have attended required information security training, and notifying departmental computer system administrators and Information Technology Services (ITS) when employees no longer require access due to reassignment or termination.

2.7. College-Wide Responsibilities

All breaches of information security must be reported immediately to campus safety and security office or the IT department accordance with the procedures listed in the NORTHERN Information Security Program.

3. Compliance by Service Providers

Service providers and/or contractors who provide services that may allow them to access protected information must comply with the GLBA safeguard requirements, the College's Information Security Program, and applicable College policies listed herein. The College Purchasing Department is responsible for reviewing prospective service providers and/or contractors to ensure they have and will maintain appropriate safeguards for protected information.

4. Monitoring and Testing

The Director of Information Technology will regularly monitor the Northern Information Security Program and periodically test the required and recommended safeguards. Based on these assessments, the Director of Information Technology will work with all appropriate individuals to implement, correct, design, or improve safeguards.

5. Evaluation and Adjustment

The Director of Information Technology is responsible for adjusting the Northern Information Security Program to ensure that the required and recommended administrative, physical, and technical safeguards are appropriate to the College's size and complexity, the nature and scope of its activities, and the sensitivity of the data and information the College handles.

INFORMATION TECHNOLOGY (IT) GOVERNANCE

1. General

It is critical that the College's information technology (IT) resources, applications, and manpower be managed in a manner that enables the College to apply new technologies and adopt new processes effectively while enhancing and encouraging the innovation required for the College to excel in all aspects of its mission. To accomplish this goal, the following IT governance framework has been developed based on a collaborative model that includes formal input, review, and approval processes for decision making. This policy describes this framework and defines the roles and responsibilities of individuals and groups involved with IT governance to ensure effective input and decision-making pertaining to IT policies, standards, guidelines, processes, and procedures.

1.1. Information Technology Governed by this Policy

The term IT is applicable to a wide array of technology systems used at Northern, and for the purposes of this policy includes but is not limited to:

- Telecommunications and facilities infrastructure (e.g. voice and data networks and supporting cable plant).
- Computing (e.g. servers and development environments for productivity and high performance computing).
- Enterprise-wide applications and user services (e.g. Banner).
- Instructional technology (e.g. classroom media systems and services, distance learning).
- Video (e.g. CATV, video applications on the network, security video).
- Peripheral technologies (e.g. printing and scanning).

2. Roles and Responsibilities

Roles and responsibilities for the individuals and groups involved with IT Governance at NORTHERN are described in the following sections.

2.1. Northern IT Director

The IT Director provides leadership and direction for the College's shared information systems to include institution-wide strategic planning and budgeting for information technologies. The IT Director also oversees coordination of all IT-related functions across the College.

3. Overview of IT Policies, Standards, Guidelines, Processes, and Procedures

Policies, standards, guidelines, processes and procedures take a tiered approach to defining IT principles and providing IT-related direction to the College. The table below defines the differing levels of scope, authority, and compliance requirements for each category.

	Scope	Approval	Communication	Compliance
IT Policies	College-wide, high-level policy	Board of Regents	All faculty and staff and students where applicable	Violation could result in discharge or dismissal
IT Standards	College-wide or limited to a IT function-technically specific	President	All affected faculty, staff, and students	Violation could result in system damage, loss of IT privileges, and/or disciplinary action
IT Guidelines	College-wide or limited to a IT function-technically specific	President	All affected faculty, staff, and students	Violation could negatively impact performance
IT Processes & Procedures	Associated with an IT application or process-technically specific	Northern IT Director	Departmental faculty or staff responsible for IT application or process	Violation could result in incorrect results or outcomes

4. Northern IT Policies

Northern IT policies are designed to provide the College community with unifying statements that describe fundamental IT principles, the reasoning behind the principles, and institutional procedures necessary for implementation. They help ensure compliance with applicable laws and regulations, enhance the College's mission, promote operational efficiencies, and/or reduce institutional risk.

4.1. Development

The development of effective policy statements requires both input from individuals who have extensive knowledge on the subject matter and input from individuals affected by the policy. Anyone wishing to propose an IT policy statement should send their request to the Northern IT Cabinet. If the Cabinet determines a need for a specific policy, it will assign individuals most closely involved with the subject matter to work with the Northern Policy Office to develop a preliminary draft. The preliminary draft will be reviewed by the IT Managers Council and then sent to the IT Agents Networking Group for comment. The Networking Group will forward their comments to the IT Managers Council for consideration. After the Council's review, the proposed policy is sent to the

IT Cabinet and the IT Governance Council for endorsement. After endorsement, the Northern Policy Office will follow standard Northern protocol for approval of institutional policy. This protocol includes review by key areas selected based on the nature of the proposed policy, Deans Council, the President's Executive Cabinet, and the campus as a whole.

4.2. Approval and Communication

All Northern IT policies must be approved by the President in writing before distribution.

Upon approval by the President the campus is notified of the new policy via email. Information concerning the policy will also be posted on the IT Director website.

4.3. Compliance

Northern IT policies contain governing principles that mandate or constrain actions and have College-wide application. The policy will state applicability to students, staff, faculty, and/or visitors and compliance is mandatory. If exceptions are allowed, the authority and procedure for requesting an exception will be delineated in the policy. Individuals who fail to comply with College policy will be subject to disciplinary action up to and including discharge or dismissal from the College. Violations of IT policies should be reported to the Office of the IT Director.

4.4. Review and Revision

IT policies will be reviewed by the Policy & Procedure Committee periodically to ensure policies are up-to-date and meeting the needs of the College.

5. IT Standards

Northern IT standards are based on industry best practices designed to ensure that IT resources are effectively managed in support of the College's mission of education, research, and public service. IT standards define procedures, processes, and practices designed to provide an efficient, effective IT system; protect confidential information; minimize security risks; ensure compliance with federal and state laws and regulations, and facilitate an open, interoperable, accessible IT infrastructure that meets the needs of students, faculty, staff, and the College community.

5.1. Development

To ensure that IT standards effectively support the mission of the College and meet the needs of the College community, development of IT standards requires a broad base of participation and involvement of subject matter experts. Draft standards will be developed by the IT Managers Council and then sent to the IT Agents Networking Group for review and comment. The Networking Group will forward their comments to the IT Managers Council for consideration. The Council will publish the proposed standard on the IT Director website and solicit comments from the campus. The IT Managers Council will update the standard based on campus comment and submit it to the IT Cabinet for review.

5.2. Approval and Communication

IT standards must be approved by the IT Director in writing prior to distribution. Upon approval, ITS will notify all individuals impacted by the standard prior to its effective date and post the standard on the IT Director website. When a new IT standard is issued, the standard will indicate the timeframe for compliance, based on but not limited to, criticality, funding limitations, and/or equipment replacement cycles.

5.3. Compliance

The type of technology addressed in the standard will determine the groups or individuals required to comply with the standard. Some standards such as password standards will apply to all users, whereas others may apply only to system administrators. Each standard will define those individuals who are required to comply with the standard. Failure to comply with a standard may damage a system, risk security, result in loss of IT privileges, and/or disciplinary action. To request an exception to an IT standard, submit a written justification to the IT Director. Violations of IT standards should be reported to the Office of the IT Director.

6. IT Guidelines

IT guidelines are directives and specifications, similar to standards, but advisory in nature. In essence, IT guidelines constitute recommendations that are not binding; however, it should be noted that failure to comply with IT guidelines may result in damage to a system and/or inefficient processes.

6.1. Development

IT guidelines are developed by IT personnel in consultation with applicable users and based on industry practices.

6.2. Approval and Communication

IT guidelines must be approved by the IT Director in writing. Upon approval, the IT Director's Office will notify all individuals impacted by the guidelines and post the guidelines on the IT Director's website.

6.3. Compliance

IT guidelines are not mandatory, but failure to follow applicable IT guidelines may result in less effective system performance and may negatively impact an individual's job or academic performance.

7. IT Processes and Procedures

IT processes and procedures provide electronic and manual mechanisms for IT-related functions or job duties.

7.1. Development

IT processes and procedures are developed by IT personnel in conjunction with applicable administrative personnel and are generally developed at the departmental and unit levels.

7.2 Approval and Communication

IT processes and procedures are usually designed in the course of application development and are approved as part of the overall project approval. These processes and procedures are documented in accordance with industry standards and communicated in conjunction with the associated project.

7.3. Compliance

Compliance with IT processes and procedures is critical to the correct functioning of the selected application. Any problems or issues associated with an IT process or procedure should be reported to the IT Director.

7.4. Review and Revision

IT processes and procedures are reviewed periodically for applicability and accuracy and updated as required in accordance with the associated application approval protocols.

8. Policies Establishment

Departmental IT Policies, Standards, Guidelines, Processes, and Procedures Colleges and departments may establish additional departmental IT policies, standards, guidelines, and processes provided they comply with College IT policies, standards, guidelines, and processes and are documented and communicated to departmental employees.