2520
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
"Identify Theft Protection Program" Policy 2040
"Information Security" Policy 2550
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 developing, maintaining and executing backup, off-site storage and disaster recovery procedures for computerized College information.

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 non-compliance 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.