Policy & Procedure No. 7.010

Nunez Community College

Title: Information Security Policy

Effective Date: 11-9-2018

Last Revision Date: 2015, 2018
Cancellation:

Department/Office: Information Technology

PURPOSE

Computer information systems and networks are an integral part of business at Nunez Community College. The College has made substantial investment in human and financial resources to create these systems.

The enclosed policies and directives have been established in order to

- Protect these resources;
- Safeguard the information contained within these systems;
- Reduce business and legal risk; and

Protect the integrity of the college, as well as the community it serves

SCOPE

This policy applies to full-time employees, part-time employees and interns (student workers).

POLICY

Administration

The IT Director or designee is responsible for the administration of this policy.

Contents

The topics covered in the document include the following:

- Communication
- Statement of responsibility

- The internet
- Computer Viruses
- Access codes and passwords
- Physical security
- Copyrights and license agreements
- PII (Personal Identifiable Information)

Communication

All policies and procedures will be communicated to all responsible parties within 24 hours of a change that has been authorized by the Chancellor's Council or authorized administrator in the form of electronic mail (email). A copy of the updated policy/procedure will be maintained by the appropriate department head; general policy/procedure changes will be maintained by the Assessment and Compliance Officer. Communication will continue on an on-going basis as the college adapts to the mandates presented by the LCTCS and other authoritative state agencies.

Statement of Responsibility

All employees of Nunez Community College are required to read the following Information Security Policy. They must sign the attached form indicating they have read and understand their responsibilities regarding the electronic equipment that is made available for the performance of their duties. The completed form must be forwarded to the IT Director or his/her designee.

Manager Responsibilities

Managers and Departmental Supervisors Must:

1. Ensure that all appropriate personnel are aware of, and comply with, this policy; and
2. Create appropriate performance standards, control practices and procedures designed to provide reasonable assurance that all employees observe this policy.

Office of Information Technology Responsibilities:

IT Director or Designee Must:

1. Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policy directives; and

2. Provide appropriate support and guidance to assist employees to fulfill their responsibilities under the directive.

The Internet and E-mail

The Internet is a very large, publicly accessible network that has millions of connected users and organizations worldwide. One popular feature of the Internet is e-mail.

Policy

Access to the Internet is provided to employees for the benefit of Nunez Community College and its students. Employees are able to connect to a variety of business information resources around the world.

Conversely, the Internet is also replete with risks and inappropriate material. To ensure that all employees are responsible and productive Internet users and to protect the College's interests, the following guidelines have been established for using the Internet and e-mail.

Acceptable Use

Employees using the Internet are representing the College. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner, and that such use does not interfere with the College's normal operations and the performance of their jobs. Examples (though not the totality) of acceptable use are the following:

- Using Web browsers to obtain business information from commercial Web sites.
- Accessing databases for information as needed.
- Using e-mail for business contacts.
- Updating College-related social media pages.

Unacceptable Use

Employees must not use the Internet for purposes that are illegal, unethical, harmful to the College, or nonproductive. Such actions could constitute malfeasance, which is a prosecutable offense. Examples (though not the totality) of unacceptable use are as follows:

- Sending or forwarding chain e-mail (i.e., messages containing instructions to forward the message to others);

- Broadcasting e-mail (i.e. sending the same message to more than 10 recipients or more than one distribution list that is not College business related);
- Conducting a personal business using College resources;
- Making personal purchases, playing games, chatting, etc.; and
- Transmitting any content that is offensive, harassing, or fraudulent.

Downloads

File downloads from the Internet are not permitted unless specifically authorized in writing by the IT Manager or designee. This includes streaming audio (ITunes, Spinner, Real Audio, etc.), music downloads (Napster, Lime wire, etc.), and chat programs (AOL instant messenger, Yahoo messenger, Facebook messenger, etc.). **In addition, tool bars are not permitted for downloading as they have been found to cause communication issues when using the Banner software suite as well other mission critical software.**

Copyrights

Employees using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by the College and/or legal action by the copyright owner.

Monitoring

All messages created, sent, or retrieved over the Internet are the property of the College and *may be regarded as public information.* Nunez Community College reserves the right to access the contents of any messages sent over its facilities if the College believes, in its sole judgment, that it has a business need to do so.

All Communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

********This means don't put anything into your e-mail messages that you wouldn't want to see on the front page of the newspaper or be required to explain in a court of law.*********

Computer Viruses

Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can cause destruction of College resources.

Background

It is important to know that:

- Computer viruses are much easier to prevent than to cure; and
- Defense against computer viruses includes protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus scanning software.
-

Information Technology Department Responsibilities

The Information Technology Department shall:

1. Install and maintain appropriate antivirus software on all computers; and
2. Respond to all virus attacks and destroy any viruses or malicious software detected.

Employee Responsibilities

These directives apply to all employees, including student workers:

1. Employees shall not knowingly introduce a computer virus into the College computers
2. Employees shall not utilize flash/jump drives of unknown origin;
3. Incoming flash/jump drives shall be scanned of viruses before they are utilized
4. Any associate who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and notify the IT Manager or Designee.

******Employees must NEVER open documents or e-mailed links that are suspicious or of unknown origin! Contact Information Technology if you cannot quarantine or scan the document/link yourself.******

Access codes and passwords

The confidentiality and integrity of data stored on College computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties. All employees accessing the campus network or email system will be issued a unique username or password which are to be kept confidential and not shared with other individuals; a record of user ID's will be maintained in the various campus systems such as AD (Active Directory), the Email administrative console and Banner system. An ID will

only be issued to an employee once Human Resources has verified the individual is part of the Nunez staff; in the event of user's name change, Human Resources will notify the IT department within 24 hours to make the appropriate changes within the campus systems. If an employee changes departments or is terminated/leaves, Human Resources will contact the IT department within 24 hours to change or terminate system access (this includes on campus systems and Banner).

In regards to Banner access, User ID's are created during the HR employee setup process; ID's and passwords ARE NOT manually created by the IT department. The campus Banner security administrator DOES NOT authorize Banner security requests; the security administrator merely processes security forms based on the authorization (or denial) by the respective campus Banner admins (ex: Finance, Student Affairs, Financial Aid, etc.) Changes in Banner security access are processed by the campus Banner Security only after those changes have been reviewed by the respective campus authorizers and marked for processing; no additional access (INB) will be granted if the campus approver does not approve the security request. Banner access is terminated upon receipt of notification from HR within 24 hours or when the campus security administrator receives the termed employee report from the system office.

Information Technology Department Responsibilities:

The IT director or designee shall be responsible for the administration of access controls to the College computer systems. The IT Director or designee will process adds, deletions, and changes upon receipt of written request from the end user's supervisor.

Deletions may be processed by an oral request prior to reception of the written request. The IT Director or designee will maintain a list of administrative access codes and passwords and store this list in a secure area.

The IT Director or designee is responsible for reporting checked out mobile equipment to the Property Department and also reporting the equipment's return.

The IT Director or designee will disable accounts for users who are absent for extended periods of time. Upon request of the employee's manager or supervisor, the account will be reactivated.

Employee Responsibilities

Each Nunez Community College employee:

1. Shall be responsible for all computer transactions that are made with his/her User ID and password;

2. Shall notify the Office of Information Technology immediately if it is suspected that others may have knowledge of their password and the Office of Information Technology will issue a replacement;
3. Shall not disclose passwords to others for any purpose. Passwords should not be on public display or recorded where they may be easily obtained;
4. Will change passwords every 30 days as mandated by the LCTCS;
5. Should use passwords that will not be easily guessed by others;
6. Should lock a computer when leaving a workstation unattended (users MUST log out of the student information system before performing this action); and
7. Will lock their computer at the end of the business day.

Supervisor's Responsibility

Managers and supervisors must notify the IT Director or designee, in writing, of any new employees that include the following information:

1. Full Name
2. Room Number
3. Phone Number
4. Title
5. Program Access Rights (i.e., E-mail, Fx-Scholar, LoLA, etc.)

Managers and supervisors will notify the IT Manager or designee, promptly, whenever an employee leaves the College or transfers to another department so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

Human Resources Responsibility

The Human Resources Department will notify the Office of Information Technology at least monthly of associate hires, transfers, and terminations. Involuntary terminations must be reported concurrent with the termination.

Physical Security

It is college policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access and environmental hazards.

Employee Responsibilities

The directives below apply to all employees, including student workers:

1. Flash/jump drives should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up. In addition, drives containing sensitive data should also be properly encrypted, as per LCTCS guidelines.

2. Flash/jump drives should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.

3. Critical computer equipment (such as file servers), must be protected by an uninterruptible power supply (UPS). Other computer equipment should be protected by a surge suppressor.

4. Environmental hazards to hardware such as food, liquids, high or low humidity, and extreme heat or cold should be avoided.

5. Since the IT Director or designee is responsible for all equipment installations, connections, modifications, and relocations, employees are not to perform these activities. This does not apply to temporary moves of portable computers for which an initial connection has been set up by the Office of Information Technology.

6. Employees shall not take shared portable equipment such as laptop computers off the premises without the informed consent of their departmental supervisor or manager. Employees that have been authorized to utilize portable equipment must fill out the appropriate paperwork in the Office of Information Technology whom will then forward a copy to the Property Department.

7. Software that is not licensed and maintained by the Office of Information Technology must not be installed or maintained on any College electronic/computer equipment. Systems found to be out of compliance with the College guidelines will be reloaded which could incur loss of user data.

8. All data that is stored on the local system must be stored in the "My Documents" folder; this folder is automatically backed up to the U: during maintenance each night. In the event that a system must be reloaded, any data not stored in the "My Documents" folder may be lost.

9. For optimal performance of the system, computer settings (display, network, printers, etc.) should not be altered

10. Equipment that is not the property of Nunez Community College should not be attached to the campus-wide network.

11. Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may result.

PII (Personal Identifiable Information)

It is the responsibility of ALL Nunez employees (full time, faculty, adjunct and student workers) to protect Personal Identifiable Information (PII). The federal government defines PII as:

"information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

Nunez employees are not to divulge PII to any 3rd party organization or entity outside of the college nor internally; in regards to Banner, students/employees should only be referred to by their unique ID or L number provided by Banner in any and all correspondence.

Enforcement Procedure

The Office of Information Technology will conduct unscheduled audits of all Nunez Community College Departments and labs to ensure all areas are in compliance with this security policy. In the event a violation is found, the following steps will be executed, depending on the severity of the offense. Other actions 'may' be deemed necessary:

1. Upon a finding of a first time violation, the employee is issued a written warning by the IT Director or designee.
2. Upon a finding of a second time violation, the employee is issued a written warning by the IT Director or designee and the user's supervisor is cc'd the warning.
3. Upon the finding of a third violation, the employee's network and e-mail access are suspended; the Director of Human Resources, as well as the user's supervisor, are contacted to discuss further disciplinary measures.

Mobile Technology Check Out

Introduction

The Office of Information Technology has in its possession several mobile technology pieces (Laptops, etc.) that can be checked out in the event an employee needs one to conduct Nunez- related business off campus.

Check Out Procedure

1. Employee must transmit an e-mail to the Information Technology Director or designee requesting the use of mobile property and provide justification for the temporary acquisition.
2. The Information Technology Director or designee will either approve or deny the request based on on-hand inventory available, employee justification, etc. The employee will be notified via e-mail the approval or denial of their request.
3. In the event a request is granted, the employee agrees to the following:
    a. The employee is responsible for the equipment in his/her possession, including the security of the unit when not in use.
    b. The unit will ONLY be used to conduct assigned job duties for Nunez Community College.
    c. The employee WILL NOT load 3rd party software onto the unit without the permission of the Office of Information Technology.
    d. The employee will return the unit to the Office of Information Technology within the timeframe specified by Information Technology staff; upon receiving notification of maintenance or inventory processing, the employee will return the unit within a 48- hour period. If the employee does not return the unit within the specified time frame, their network access and e-mail will be deactivated until the unit is returned and their supervisor notified.
    e. If the unit is lost, stolen or damaged due to negligence, ***the replacement value of the laptop 'may' be deducted from the employee's salary via payroll.***
4. Once an employee is issued mobile equipment, the IT office will notify the property department via e-mail of the following: Employee the equipment was issued to, type of equipment, tag number of equipment, check-out timeframe. The IT office will also notify the property department via e-mail when the checked out equipment has been returned.

Consequences of Actions

Employees who are found to be in violation of this policy will be subject to the Progressive Discipline steps outlined in the Employee Handbook. Egregious actions which result in actual harm to any other employee, any student, or to the College, its representatives or reputation, could result in immediate disciplinary action, up to and including termination of employment

Violations

Violations may result in the disciplinary action in accordance with College policy. Failure to observe these guidelines may result in disciplinary action by the College, depending upon the type and severity of the violation, whether it causes any liability or loss to the college, and/or the presence of any repeated violation(s).

X	Reviewing Council/Entity	Review Date	Effective Date
X	Office of Information Technology	10-2018	11-9-2018
X	College Compliance Committee	11-2018	11-9-2018
X	Chancellor's Council	11-9-2018	11-9-2018

Policy Referenced:

Distribution: Distributed Electronically via College's Internet 1-14-2019

Chancellor's Signature/Approval

SIGNATURE:_____ DATE: 11-15-2018

Tina M. Tinney, Ed.D.
Chancellor