# College of Menominee Nation

## Information Technology Security Use Policy

*Prepared by Renita Wilber*

**August 25, 2009**

# Introduction

Computer information systems and networks are an integral part of business at the College of Menominee Nation (CMN). The organization has made a substantial investment in human and financial resources to create these systems.

Only those computer resources designated as **Library Public Use** are accessible and can be used by the public. College of Menominee Nation Information Security Policy will apply to public users

The enclosed policies and directives have been established in order to:

- Protect this investment.
- Safeguard the information contained within these systems.
- Reduce business and legal risk.
- Protect the good name of the organization.

# Violations

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

# Administration

The Information Technology (IT) Director is responsible for the administration of this policy.

# Contents

The topics covered in this document include:



# Statement of responsibility

General responsibilities pertaining to this policy are set forth in this section. The following sections list additional specific responsibilities.

## *IT Staff responsibilities*

The IT Staff must:

1. Ensure that all appropriate personnel and students are aware of and comply with this policy.

2. Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees/students observe this policy.

## *IT Director Responsibilities*

The IT Director must:

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

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

# The Internet, e-mail, and wireless

This policy pertains to internet, email and wireless use on any computer connected to the CMN network or placed in any CMN educational environment.

## *Policy*

Access to the Internet is provided to employees and students for the benefit of College of Menominee Nation and its students. Employees and students are able to connect to a variety of educational resources around the world.

Unfortunately, computers connected to the Internet also face risks associated with computer viruses and data security, and users can easily and in some cases inadvertently download material that is inappropriate to the educational, business or workplace setting. To ensure that all employees and students are responsible and productive Internet users and to protect the organization's interests the following guidelines have been established for using the Internet, e-mail and wireless.

## *Acceptable use*

Employees and students using the Internet are representing the organization. Employees and students are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

- Using Web browsers to obtain educational information from educational Web sites.
- Accessing databases for information as needed.
- Using e-mail for College of Menominee Nation business contacts.

## *Unacceptable use*

Employees and students must not use the Internet for purposes that are illegal, unethical, harmful to the organization, or nonproductive. Examples of unacceptable use are:

- Broadcasting e-mail, i.e., spam.
- Transmitting any content that is offensive, harassing, slandering or fraudulent.
- Non-instructional/Non-business chat rooms.
- Destruction of or damage to equipment, software, or data belonging to the College or others.
- Disruption or unauthorized monitoring of electronic communications.
- Use of the College's trademarks, logos, insignia, or copyrights without prior approval.
- Use of computing facilities for private business purposes unrelated to the mission of the College or to College life.
- Violation of software license agreements.
- Displaying or sending obscene, pornographic, sexually explicit, or offensive material.
- Displaying or sending material that is contrary to the mission or values of the College.
- Peer-to-Peer (P2P) file sharing programs for non instructional use.

## *Downloads*

Downloading or installing unauthorized software of any kind to computer hard drives is forbidden. Files or programs may be downloaded to removable media and designated file shares as directed by College faculty or staff.

## *Employee and student responsibilities*

An employee or student who uses the Internet or Internet e-mail shall:

1. Ensure that the use of the Internet does not interfere with his/her productivity.

2. Be responsible for the content of all text, audio, or images that (s)he places or sends over the Internet. All communications should have the employee's/student's name attached.

3. Not transmit copyrighted materials without permission.

4. Know and abide by all applicable College of Menominee Nation policies dealing with security and confidentiality of organization records.

5. Avoid transmission of information that is protected by Family Educational Rights & Privacy Act (FERPA). If it is necessary to transmit such information, employees are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate use.

## *Copyrights*

Employees and students using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs i.e. shareware 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 organization and/or legal action by the copyright owner.

## *Monitoring*

All messages created, sent, or retrieved over the Internet are the property of the organization and *may be regarded as public information* College of Menominee Nation reserves the right to access the contents of any messages sent over its facilities if the organization 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 organizational resources.

## *Background*

It is important to know that:

- Computer viruses are much easier to prevent than to cure.

· Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

## IT Staff *responsibilities*

IT staff shall:

1. Install and maintain appropriate antivirus software on all College of Menominee Nation owned computers.

2. Respond to all virus attacks, destroy any virus detected, and document each incident.

## *Employee/Student/General Public responsibilities*

These directives apply to all employees and students:

1. No one shall knowingly introduce a computer virus into organizational computers.

2. No one shall load storage media of unknown origin. (Storage media is recording (storing) information (data)).

3. Incoming storage media shall be scanned for viruses before they are read.

4. Any person who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and call the IT help desk.

# Access codes and passwords

The confidentiality and integrity of data stored on organization computer systems must be protected by access controls to ensure that only authorized persons have access. This access shall be restricted to only those capabilities that are appropriate to each person's duties.

## *IT Director Responsibilities*

The IT Director shall be responsible for the administration of access controls to all organization computer systems. The IT Staff will process adds, deletions, and changes upon receipt of a written request from the Human Resources Department**.**

Deletions may be processed by an oral request prior to reception of the written request. The IT Director and his/her staff will maintain a list of administrative access codes and passwords and keep this list in a secure area.

## *Employee/Student Responsibilities*

Each employee/Student:

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

2. Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that others may know them. Passwords should not be recorded where they may be easily obtained.

3. Should log out when leaving a workstation for an extended period.

## *Human Resources Department Responsibility*

Human Resource Department should notify the IT Director or his/her designee promptly whenever an employee leaves the organization or transfers to another department so that his/her access can be revoked/changed. Involuntary terminations must be reported concurrent with the termination.

# Physical security

It is organizational 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:

1. Storage media should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.

2. Storage media should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.

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

4. Since the IT Department Staff is responsible for all equipment installations, disconnections, 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 IT Department.

5. Employees shall not take College of Menominee Nation owned equipment out of the building without completing the appropriate paperwork from the IT Department. Informed consent means that the manager knows what equipment is leaving, what data is on it, and for what purpose it will be used.

6. Employees should exercise reasonable 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.

7. All non CMN wireless access points, network devices, and computers are not allowed to connect to the CMN network without prior approval from the IT Director.

## *Computer work areas:*

The directives below apply to all employees and students:

1. No food or drinks allowed in any computer lab, library and resource rooms by anyone. This is strictly enforced and lab privileges can be revoked.

2. Students must have ID card available at all times to verify student enrollment.

3. Only software owned by College of Menominee Nation may be used in College of Menominee Nation computers. Installation of software or hardware is strictly prohibited.

4. All individuals using the computer lab, library and resource rooms must respect the rights and needs of other lab users.

5. Disruptive behavior of any type is not allowed.

6. The computer lab, library and resource rooms must be maintained as a quiet area.

7. No children under the age of 18 are allowed in the computer labs, even if supervised by a parent, unless permission has been granted by a member of the CMN staff or faculty. Once permission is granted, a member of the CMN staff or faculty must be in the computer lab while the child is present.

8. Never unplug any computers or cables unless instructed to do so by IT Staff.

9. Do not disrupt classes using the computer labs.

10. College of Menominee Nation has the authority to refuse admittance or to expel anyone for violation of these policies.

# Copyrights and license agreements

It is College of Menominee Nation policy to comply with all laws regarding intellectual property.

## *Legal reference*

College of Menominee Nation and its employees are legally bound to comply with the Federal Copyright Act (Title 17 of the U. S. Code) and all proprietary software license agreements. Noncompliance can expose College Of Menominee Nation and the responsible employee(s) to civil and/or criminal penalties.

## *Scope*

This directive applies to all software that is owned by College of Menominee Nation, licensed to College of Menominee Nation, or developed using College of Menominee Nation resources by employees or vendors.

## *IT Department Staff responsibilities*

The IT Department Staff will:

1. Maintain records of software licenses owned by College of Menominee Nation.

2. Periodically (at least annually) scan organization computers to verify that only authorized software is installed.

## *Employee/Student responsibilities*

Employees/Students shall not install or copy software that is not licensed to or owned by College of Menominee Nation on the organization’s computers.

## *Civil penalties*

Violations of copyright law expose the organization and the responsible employee(s) to the following civil penalties:

- Liability for damages suffered by the copyright owner
- Profits that are attributable to the copying
- Fines up to $100,000 for each illegal copy

## *Criminal penalties*

Violations of copyright law that are committed “willfully and for purposes of commercial advantage or private financial gain (Title 18 Section 2319(b)),” expose the organization and the employee(s) responsible to the following criminal penalties:

- Fines up to $250,000 for each illegal copy
- Jail terms of up to five years

# Acknowledgment of Information Technology Security Use Policy

This form is used to acknowledge receipt of, and compliance with, the College of Menominee Nation Information Technology Security Use Policy.

## Procedure

Complete the following steps:

1. Read the Information Technology Security Use Policy.
2. Sign and date in the spaces provided below.
3. Return this page only to the (IT Director).

## Glossary of Terms

**Chat Room** : The name given to a place or page in a Web site or online service where people can "chat" with each other by typing messages which are displayed almost instantly on the screens of others who are in the "chat room."

**FERPA:** Family Educational Rights & Privacy Act

**Internet**: The Internet is a very large, publicly accessible network that has millions of connected users and organizations worldwide.

**IT:** Information Technology

**Organization:** College of Menominee Nation (CMN).

**Peer-to-Peer (P2P):** A commonly used protocol for downloading software, music or other files with other ordinary users on the Internet. P2P is often used to obtain freeware, shareware, and bootleg software. P2P exchange is often made practical through web sites that act as clearinghouses listing people who have or want something. One of the most famous of these was Napster.

**Shareware :** Software that you can try before you buy. It's distributed through on-line services, and user groups. You're allowed to try it out and give copies to others, but if you want to keep using it, you must pay the registration fee.

**Spam:** Unsolicited "junk" e-mail sent to large numbers of people to promote products or services.

**Storage Media:** Is a device used to record (store) information (data). Types of storage media: Compact Disk (CD), floppy disk, USB Flash Drive (Thumb Drive), Digital Video Disk (DVD).

**Unauthorized Software:** Unlicensed or unapproved software. Examples include but are not limited to games, web shots, instant messengers, shareware, etc.