Turtle Mountain Community College
Information Technology Appropriate Use Policy

Responsible Office Information Technology	**Effective Date**	07/06/2011
Responsible Official IT Director	**Revised**	08/21/2012

Scope

This policy applies to all users of IT systems, including but not limited to students, faculty, and staff. It applies to the use of all IT systems. These include systems, networks, and facilities administered by the IT Department, as well as those administered by individual departments, laboratories, and other college-based entities.

Policy Statement

The purpose of this policy is to ensure an information technology infrastructure that promotes the basic mission of the college in teaching, learning, research, and administration. In particular, this policy aims to promote the following goals:

- To ensure the integrity, reliability, availability, and superior performance of IT systems.
- To ensure that IT systems are used for their intended purposes.
- To establish processes for addressing policy violations and sanctions for violators.

Policies and Guidelines

Unacceptable Use:

Definition:

Use of institutional computers, network, and internet services is a privilege, not a right.
All users are required to comply with this policy and the accompanying rules.

Policy Statement:

The following rules are intended to provide general guidelines and examples of prohibited use. Failure to comply with these rules may result in loss of computer and internet access privileges, disciplinary action, and/or legal action.

- All users shall have no expectation of privacy regarding computer files, email or internet usage. Turtle Mountain Community College reserves the right to monitor all computer files, email, and internet usage without prior notice.
- All users may not attempt to gain unauthorized access to any other computer system or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing."

- All users will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means.
- All users are not allowed to download, copy, or install any games or unauthorized software on college computers. Any unauthorized software and games, if found in the college computers, will be removed by college IT Department.
- All users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language. Restrictions against inappropriate language apply to public messages, private messages, and material posted on social media sites.
- All users will not post private information about another person.
- All users will not engage in personal attacks, including prejudicial or discriminatory attacks.
- All users will not knowingly or recklessly post false or defamatory information about a person or organization.

Email Policy:

Definition:

Use of email by staff, faculty, and students is permitted and encouraged where such use supports the goals and objectives of the institution.

Policy Statement:

Users of TMCC's email services are expected to act in accordance with the following policies and with professional and personal courtesy and conduct.

- Email is an official means of communication at TMCC. The institution may send communications to users by e-mail and has the right to expect that those communications will be received and read in a timely fashion. Information sent via e-mail has the same importance and needs to be responded to in the same manner as information sent in other ways.
- The Information Technology personnel will assign all users an official institution e-mail address. It is to this address that the institution will send all official e-mail communications.
- Any emails that discriminate against employees by virtue of any protected classification including race, gender, nationality, religion, and so forth, will be dealt with according to the harassment policy.
- All users are expected to read and properly dispose of e-mail promptly. Prompt disposal of e-mail is necessary to manage storage space on the institutional e-mail system. Disposal may include deletion, filing into alternate folders on the institutional servers, or moving the e-mail onto the user's own computer. The institution reserves the right to purge mail from accounts. Prior notification will be given if that notification is feasible and practical to allow users time to save messages.
- All users of electronic communication, including e-mail, need to realize that communication of this type usually leaves traces as to its origin and destination as well as its content. The simple deletion of e-mail or other electronic files does not remove these traces and the file or e-mail is often recoverable for some time after deletion. Further, users need to realize that the institution makes regular archival copies of all e-mail to ensure the system's integrity and that these archives exist for some time. Therefore, although TMCC's e-mail system and governing policies may grant some privacy to users e-mail, users should treat all e-mail as if they were public documents.

- In some cases a user may wish to configure his or her TMCC account to forward e-mail to another address. The user takes full responsibility for the correct configuration of that forwarding. The institution takes no responsibility for the handling of e-mail in this fashion. The use of automatic e-mail forwarding does not absolve the user from the responsibilities associated with e-mail sent to the user's official e-mail address. The institution or individual schools may forbid the automatic forwarding of e-mail in cases where it is found to be problematic. Additionally, the institution may delete e-mail forwarding or other automated e-mail handling rules that cause system problems without prior notification.
- Send or attempt to send, spam of any kind.
- The institution uses spam filtering tools to help control unwanted email. The institution will continue to stay up-to-date with the latest spam filtering techniques and will adjust its own processes when warranted. However, no current spam filtering technique is completely effective and they will let mail through that should be blocked and occasionally block e-mail that should be delivered. Moreover, each person's definition of spam is unique. Given that, users should expect that on rare occasions, legitimate e-mail may be blocked from delivery. If this happens please contact the IT Department for further assistance.
- Once an employee has resigned/terminated or a student has graduated/withdrew, they will have two weeks to save any email. After the two weeks the account will be deleted.
- Mass e-mails are defined as messages sent to all students, all staff, all faculty, when individual recipient addressees are not defined. IT manages e-mail distribution lists of current staff, faculty, and students. There is no opt-out provision for these lists. If you need to attach a large file please contact the IT Department for alternate methods of distribution.
- Keep in mind that the TMCC owns any communication sent via email or that is stored on institutional equipment. Administration and other authorized staff have the right to access any material in your email or on your computer at any time. Please do not consider your electronic communication, storage or access to be private if it is created or stored at work.

Network Privileges Policy

Definition:

Individuals who are eligible to receive access to network services.

Policy Statement:

The following users are identified as eligible to receive network services from TMCC. Any applicant for network not described below should be referred to the IT Department, who will coordinate a decision on that particular case.

- **Students:** All full-time and part-time students may receive network privileges without restriction.
- **Faculty:** All full-time faculty without restriction. Part-time faculty, faculty with temporary or cyclical appointments, and visiting faculty may receive limited network privileges.
- **Full-time regular part-time staff:** All regular, non-faculty, college employees may receive network privileges without limitations.

- **Temporary employees, visitors:** Temporary employees and visitors may receive network privileges at the request of the employing department and the assistance of the Information Technology Department.

Password Policy

Definition:

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of TMCC's entire network. As such, all TMCC staff, faculty, and students are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Policy Statement:

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

- All system-level passwords must be changed on at least a 120 day basis.
- All production system-level passwords must be changed on at least a 120 day basis.
- All user-level passwords must be changed at every 6 months.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

Guidelines:

- It must be at least eight characters in length.
- It must contain at least one alphabetic and one numeric character.
- It must be significantly different from previous passwords.
- It cannot be the same as the user ID
- It cannot include the first, middle, or last name of the person issued the user ID.
- It should not be information easily obtainable about you. This includes license plate, social security, telephone numbers, or street address.

Wireless Policy

Definition:

The purpose of this policy is to provide reliable and secure wireless network access at Turtle Mountain Community College.

Policy Statement:

This policy applies to all wireless network users at Turtle Mountain Community College.

- TMCC is solely responsible for providing wireless networking services on campus. No other department may deploy wireless network access points or other wireless service

on campus. Private wireless access points in the departments or offices are strictly prohibited.

- TMCC is responsible for maintaining a secure network and will deploy adequate security procedures to support wireless networking on campus.
- TMCC will develop a procedure for the temporary use of a wireless access point to support campus events.

Consideration:

Wireless networking has bandwidth limitations compared to the wired network. The wireless network should be viewed as augmenting the wired network, to provide more flexible network use. Applications that require large amounts of bandwidth, or are sensitive to changes in signal quality and strength may not be appropriate for wireless access.

Enforcement

Users who violate these policies may be denied access to institution computing resources and may be subject to other penalties and disciplinary action, including possible expulsion or dismissal. Alleged violations will be handled through the institution disciplinary procedures applicable to the user. The institution may suspend, block or restrict access to an account, independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of institution or other computing resources or to protect the institution from liability. The institution may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Printed Name: _____ Role: Student or Staff (Circle One)

Signature: _____ Date: _____