

TITLE: Information Technology Security**CATEGORY:** Policy**NUMBER:** C1020**PURPOSE:** To describe the policy regarding the Information Technology Security at Mohawk College.**ACCEPTABLE USE GUIDELINES**

All persons using Mohawk College's information technology resources and facilities (hereafter referred to as I.T. resources) must adhere to the *Information Technology Acceptable Use Guidelines*. These guidelines should be read in conjunction with the Information Technology Security Policy, and the Information Technology Code of Conduct for Student and Academic Clients or the Information Technology Code of Conduct for Employees and Contracted Individuals.

GUIDELINES FOR USING PERSONAL COMPUTERS AND NETWORK RESOURCES:

- Be familiar and comply with all federal and provincial laws, all College policies, such as the college's Human Rights policy, and the Information Technology (Student or Employee) Codes of Conduct.
- Comply with copyright laws and software licensing agreements. Software, which is unauthorized or illegal, may not be installed on Mohawk College servers or computers.
- Identify yourself correctly to the network when logging on, where applicable. Using someone else's account or password, or forging an account or password is strictly prohibited.
- Protect your computer, software, and files appropriately. Establish a machine (bios) password, set a password on your screen saver, and password protect sensitive or confidential data or files to prevent unauthorized users from accessing your computer, software, and files. Routine backups should also be performed to guard against the loss of information.
- Keep your accounts and passwords confidential. All users may be assigned an account and password, so there is no need to share them.
- Use College I.T. resources for college business only. Such resources may not be used for personal gain or profit, political or religious use, or commercial advertisements. Remember that all files and programs residing on a College workstation or network are the property of Mohawk College.
- Playing games, spamming of messages, broadcasting unsolicited e-mail, etc. is **an improper use of College property and a waste of valuable networking resources and is strictly prohibited.**
- Scan or ensure the necessary virus protection software is installed to scan all software and files received from others or downloaded from the internet, otherwise, you could inadvertently download, install or run any program intended to damage or place excessive loads (for example, viruses, Trojan horses, worms, etc.) on a computer system or the network. If you believe you have received a virus in an email message, for example, do not open it. Contact your LAN Administrator or the I.T. Division immediately.
- Encrypt sensitive or confidential information prior to transmitting it via the Internet. Interception of data on the Internet is elementary and common; therefore, College, proprietary, or private information should either be encrypted or sent via another method. This includes the transmission of credit card numbers, and log-in accounts and passwords.
- Make arrangements with the Director of Information Technology if you require your own personal computer equipment (including laptops), personal networking equipment (including interfaces and software), or a modem to be connected to your workstation or to the College network. Use of such equipment can degrade network performance, create security exposures and tie up needed telephone lines; therefore, requests need to be reviewed for approval. Before any equipment can be installed, an **Information Technology Hardware Registration form** must be completed and submitted to the IT Director with approval by the submitter's manager.

- Contact the applicable system administrator to gain access to a particular system. Accounts and passwords are managed by those administrators only, and access cannot be granted by an unauthorized individual.
- Use internet resources for teaching, learning, research, student life, and administration purposes only. Viewing or listening to material that is illegal, offensive, or otherwise inappropriate to the user's function is prohibited.
- Remove or make arrangements to retain all personal data and files prior to leaving the College, either upon completion of a semester or graduation (students), or termination (employees). The College will remove access to all Mohawk College I.T. resources upon such leaving.
- Understand that the Information Technology Division has the right to regularly check and monitor networking resources and facilities, and reserves the right to take any appropriate action to protect such resources and facilities.

GUIDELINES FOR USING ELECTRONIC COMMUNICATION RESOURCES (E-MAIL AND VOICE-MAIL):

- Be familiar and comply with all federal and provincial laws, all College policies, such as the college's Human Rights policy, and the Information Technology (Student or Employee) Codes of Conduct.
- Do not send or distribute messages or files of an illegal, libelous, abusive, harassing, obscene, offensive, discriminating, threatening, intimidating, or demeaning nature to any individual or group as this is strictly prohibited.
- Use College communication systems for college business only. Such resources may not be used for personal gain or profile, political or religious use, or commercial advertisements.
- Identify your official position or affiliation with Mohawk College. You may not misrepresent yourself or your intentions in any communication using College resources. Official communications must not contain information that is harmful or embarrassing to the College. Any opinions expressed by you must contain a statement that they are your opinions, and do not reflect on the College.
- Do not send or forward broadcast messages or unsolicited e-mail.
- Create an appropriate e-mail or voice-mail forwarding strategy during long periods of leave or vacation. Be sure to unsubscribe from any discussion lists before you create an e-mail auto-reply message, as not doing so creates an infinite loop of messages which causes annoyance to the list owner and complaining messages for you.
- Recognize that the College cannot secure communication systems. It is therefore recommended that you do not send confidential or sensitive data or files via e-mail unless they are encrypted.
- Protect your password for your e-mail and voice-mail systems.
- Report any suspect communications to the Director of Information Technology immediately.

GUIDELINES FOR PASSWORDS:

- Memorize your passwords. Passwords should never be written down.
- Protect your passwords from others. Never share your passwords with anyone.
- Create a password that is meaningful and easy to remember, but difficult for others to guess. It should be a minimum of six characters, preferably with numbers as well as letters. Try not to choose a password that is a proper name or a dictionary word. These are easy for hackers to decipher.
- Change your passwords every 6 to 12 months, or immediately if you suspect a hacking attempt or infiltration.

- Use a different password for each system.

Considerate and authorized use of all of Mohawk College's information technology resources and facilities will ensure suitable availability of those resources and facilities to everyone.

EMPLOYEE CODE OF CONDUCT

PREAMBLE:

Mohawk College grants the privilege of using information technology resources and facilities (hereafter referred to as I.T. resources) to students, clients and employees strictly for the purposes of learning, teaching, research, student life, and administration. While the College makes every effort to ensure network security and data integrity, individuals also have certain responsibilities, and as such are responsible for making themselves aware of the applicable laws, policies, and guidelines. All employees and other contracted individuals will abide by this *Information Technology Code of Conduct*, the Information Technology Security Policy, and the Information Technology Acceptable Use Guidelines.

GOVERNING STATUTES, REGULATIONS, AND POLICIES:

The use of Mohawk College's I.T. resources is subject to all federal and provincial laws, and to the College's applicable policies and procedures. These include, but are not limited to the following:

Federal

Canadian Bill of Rights
Copyright Act
Criminal Code of Canada

And others that may be appropriate

Provincial

Freedom of Information & Protection of Privacy Act
Human Rights Code
Libel and Slander Act

And others that may be appropriate

Mohawk College

Information Technology Security Policy (C1020 – previously Computing & Telecommunications Policy)
Information Technology Acceptable Use Guidelines (new)
World Wide Web Page Policy (C125)
Copyright (C140)
Publication of Employee Produced Material (C150)
Sale of College Generated Material and Employee Generated Material on Non-College Time (C155)
Access to Information and Privacy Act (C201)
Cellular Telephones (C211)
College Employee Information Technology Workstations (C223)
Use of College Property (C225)
Disruptive Behaviour in the Learning Environment (C229)
Freedom of Information and Protection of Individual Privacy Act Policy (C242)
Threats, Acts of Violence and Weapons Possession (C292)
Conflict of Interest, All Employees (H310)
Human Rights Policy (H320/C202)

SPECIFIC ACTIVITIES:**1. Personal Use:**

Users will **not** use Mohawk College I.T. resources for personal gain or profit, or for political or religious purposes. Resources and facilities must be specifically used for the sole purposes of teaching, learning, research, student life and administration of the College. All equipment, files or programs that reside on a College workstation, server or network are the property of the College.

2. College Access to Electronic Communications and Electronic Files:

2.1 Mohawk College endeavors to respect the right to privacy of all users; however, the College cannot guarantee confidentiality of all electronic communications. In order to develop, maintain, or repair the network and its systems, key identified staff members have special access privileges that allow them to gain access to any resources residing on the network. You are therefore cautioned to use discretion when sending or saving electronic communications.

2.2 In accordance with the **Freedom of Information and Protection of Privacy Act**, the public and authorized individuals may have access to a users' electronic records stored on College computers, subject to applicable exemption under those Acts. These records include electronic communications and visited web sites that are tracked on a user's computer.

3. Criminal Offenses:

Users will adhere to all applicable laws of Canada (federal), and Ontario (provincial). For example, the proliferation of pornographic, obscene or abusive materials, or hate literature is forbidden and is punishable by the appropriate authorities.

4. Copyright:

Users will observe copyright and software licensing agreements. For example, copying programs, data, images, audio files, etc. that are the property of another without the owner's expressed authorization, or installing or running unlicensed or illegal software, or allowing the copying, installation or running of unlicensed or illegal programs or files is forbidden and is punishable by the appropriate authorities.

5. Hacking:

5.1 Users will **not** attempt unauthorized access to computer installations inside or outside of Mohawk College using Mohawk College's I.T. resources.

5.2 Users will **not** forge or misrepresent their identity, or provide false or misleading information to gain access to I.T. resources inside or outside of Mohawk College.

5.3 Users will **not** deliberately mask the identity of an account or machine.

5.4 Users will **not** probe for loopholes or attempt to circumvent security protection schemes of hardware or software, nor engage in any activity that attempts to compromise the security of any system.

5.5 Users will **not** install or use software or other tools that allow access to others' systems, accounts or passwords.

6. Human Rights:

Users will abide by Mohawk College Human Rights Policy H320/C202.

Users will not use Mohawk College I.T. resources to transmit, display, distribute, or make available materials that are harassing or discriminatory, in keeping with the College's Human Rights policy. Illegal, libelous, abusive, obscene, threatening, intimidating or demeaning transmissions to any individual or group are also prohibited. This includes, but is not limited to, the use of electronic mail systems, and postings on electronic bulletin or message boards and web pages.

7. Wasting Information Technology Resources:

Users will **not** waste I.T. resources by playing games, spamming of messages, flooding the network, running or installing programs intended to damage or to place excessive load on a computer or the network (for example, viruses, Trojan horses, worms, etc.), or otherwise interfering with the normal operation of the network, and thus depriving other users of I.T. resources. If a user is the recipient of such activity, e.g. receiving email containing a virus, then the user must contact the I.T. Division immediately so as not to threaten or compromise the security of the College's systems or network.

8. User Privacy:

Users will **not** view, destroy, or alter the integrity of any information belonging to another user without the owner's expressed authorization. All material stored on a server or a computer or transmitted via the network is presumed to be confidential and private. This includes email messages and attached files that may have been sent in error either by the originator or a virus program. Users will not compromise the privacy of any other user by viewing or forwarding such messages or attachments when it is determined that the information was not intended to be distributed.

9. User Accounts and Passwords:

Users will **not** give their accounts or passwords to others, nor allow others to gain access to their accounts or passwords. All accounts and passwords are private and confidential.

10. Reporting Misuse:

Users must report the misuse of Mohawk College I.T. resources to the appropriate Chair, or the Director of Information Technology. Failure to do so may result in the assumption that the user who witnessed the misuse was party to the act.

11. Denial of Access After Termination:

Terminated or retired employees do **not** have access to Mohawk College I.T. resources except as specifically approved by the Director of I.T. or other authorized College official. Access to files, including any personal files, on such employees' workstations or network servers will cease on the employee's last day of work.

12. Enforcement and Consequences of Violation:

- Violation of federal or provincial laws is enforced and punishable by the appropriate federal or provincial authorities.
- Mohawk College policies and codes are the responsibility of the Board of Governors of Mohawk College and are enforced by the appropriate designate, likely the Director of Information Technology. Enforcement of the policies and codes will be shared by that appropriate individual and the Director of Human Resources. For more information see the Roles and Responsibilities section of the Mohawk College Information Security Policy.
- Violation of a Mohawk College policy or this Code of Conduct will result in any one or a combination of the following:
 - i. verbal warning(s)
 - ii. written warning(s)
 - iii. restriction or withdrawal of access to resources and facilities
 - iv. suspension
 - v. termination
 - vi. criminal or civil action

All users are also encouraged to review the Mohawk College Information Technology Acceptable Use Guidelines.

INFORMATION TECHNOLOGY SECURITY POLICY**PREAMBLE:**

Mohawk College provides computing, information, communication, and networking resources and facilities (hereafter referred to as I.T. resources) to authorized employees, students and community partners for the purposes of teaching, learning, research, student life and administration in support of the College's mission and goals. The College recognizes its responsibility, which may be shared with divisions, departments and individuals as appropriate, to ensure the security and integrity of such I.T. resources, and of all authorized users.

SECURITY POLICY STATEMENT:

No person shall knowingly breach, compromise, endanger or threaten Mohawk College's I.T. resources, attempt to do so, or allow others to do so.

DEFINITIONS:

Security: The freedom from unacceptable risk or danger, such as tampering, hacking, spreading of viruses, etc.; having confidence in the safety and protection of property.

IT resources include, but are not limited to, the following:

- local computers in classroom labs, Open Access, staff workstations, SAM stations, etc.
- corporate mainframe computers
- academic and administrative servers - corporate, departmental and workstations
- the network - College backbones, cables, routers, switches, internet access, etc.
- firewalls
- printing devices - printers, photocopiers, scanners, plotters, netports, etc.
- software packages and applications, including operating systems (purchased or built in-house)
- data - databases, files, documents, system documentation, graphics, audio, video, etc.
- communications - e-mail, voicemail, newsgroups, telephone system, fax machines, modems, etc.
- transmission of data - Electronic Data Interchange (EDI)

Authorized Users:

- all full-time and part-time employees of the College
- all active full-time and part-time students in good standing
- any other authorized person maintaining an agreed upon affiliation with the College

SCOPE OF INFORMATION TECHNOLOGY SECURITY:

This policy applies to all I.T resources which are the property of Mohawk College, whether they reside on College property or are connected to, or a part of the College's information technology infrastructure. The College reserves the right to limit or restrict access to any I.T. resource, or to any user, as deemed necessary. Since I.T. resources represent a significant monetary investment by the College, protection of these assets on all levels is paramount.

- Protection of all electronic information (e-mail, files, etc.) which are stored in the College's information systems and ensuring that information which is stored complies with applicable provincial and federal laws, including the Copyright Act, as well as principles of common decency;
- Protection of the workstation from infiltration or threat in order to secure the College's investment in hardware and software;
- Protection of the Local Area Network (LAN) (including labs and connectivity of computers within a campus) and the Wide Area Network (WAN) (connectivity of computers between campuses) from infiltration or threat in order to secure the College's investment in hardware and software, and to ensure the efficient operation of the network;
- Globally, the College must implement appropriate protection when connecting to the internet in cooperation with existing Internet Service Provider agreements.

Appropriate methods of securing I.T. resources will be implemented by the applicable College representative as defined in the **Roles & Responsibilities** section of this Policy. Security methods may include, but are not limited to, locked storage areas; installation of firewalls; data encryption; password protection for users and on servers, workstations, and sensitive files; and network monitoring devices to be used only by authorized I.T. staff.

Registration of all new hardware (servers, netports, routers, bridges, etc.) which is to be connected to the corporate network must be submitted to the Director of Information Technology to ensure that the necessary resources are available to operate and maintain the new equipment, and to ensure the appropriate security measures are in place. The "Hardware Registration Form" (Appendix A) will be completed by the department manager and forwarded to the Director of Information Technology. Installation of new workstations is usually managed by the Information Technology Division, therefore, registration of new workstations is not required unless this is not the case.

Where possible, users will be authenticated in order to assist the College in identifying authorized versus unauthorized accesses to I.T. resources. User accounts and passwords will be created and maintained, where it is feasible and reasonable to do so, in accordance with the Information Technology Acceptable Use Guidelines (Appendix B).

ROLES AND RESPONSIBILITIES:

Policy Administration:

- approval by the Board of Governors of Mohawk College under the recommendation of the President and Mohawk College Council
- implementation by all individuals (authorized users), as identified below.

Director of Information Technology:

The Director of Information Technology is responsible for the security of

- all corporate equipment, including the network and underlying infrastructure, mainframe computers, corporate servers, remote access, cabling, routers, and switches;
- the corporate internet connection;
- the hardware and software in general purpose labs including Sony labs, classroom labs, and Open Access; and
- telecommunications systems, including e-mail, newsgroups, telephone and voice mail systems

Departments and Information Custodians:

- Department managers (deans, directors, managers, chairs) are responsible for the security of hardware (which may include departmental servers and workstations), software (purchased or built in-house) and data managed by that department.
- Department managers are responsible for ensuring that authorized users are aware of and agree to the *Information Technology Security Policy* and the applicable *Information Technology Code of Conduct*, and for ensuring access to resources is appropriately removed upon termination of employees or graduation, suspension or expulsion of students.
- Department managers are responsible for maintaining their own licensing agreements and having all proper licensing documentation, for any software acquired through the department. The Information Technology division assumes responsibility for college-wide site licenses. The College's Copyright Policy must be followed.
- Regarding the security of corporate systems and data, the Director of Human Resources is responsible for the Human Resources Information System, the Registrar for the Student Information System, and the Director of Finance for the Finance System.
- The Director of College Services is responsible for the physical security of all resources and facilities.

Individuals (Authorized Users):

- All authorized users are responsible for the security of the data and files on their workstation.
- Authorized employees are responsible for conducting themselves in accordance with the Information Technology Code of Conduct for Employees and Contracted Individuals and the Information Technology Acceptable Use Guidelines, and will comply with all applicable international, federal and provincial laws.
- Authorized students are responsible for the proper care and use of I.T. resources in accordance with the Information Technology Code of Conduct for Students and Academic Clients, and the Information Technology Acceptable Use Guidelines, and will comply with all applicable international, federal and provincial laws.

EXCEPTIONS:

In order to ensure adequate security measures are in place and to guard against malicious attacks, I.T. staff are required to monitor the network, servers and networking devices. Such monitoring will not be considered a violation of international, federal and provincial laws, this Policy, or of the applicable *Information Technology Code of Conduct*.

ENFORCEMENT & CONSEQUENCES:

The College reserves the right to issue or deny a user access to any I.T. resource as deemed appropriate by the College. The department manager has the authority to limit access to departmental resources (department servers, specialty labs, workstations, etc.). The Director of Information Technology, in conjunction with the Registrar or Director of Human Resources as applicable, has the authority to limit access to corporate resources (general purpose labs, the network, corporate servers, mainframes, corporate systems and data, the internet, etc.).

Anyone found to be in violation of relevant College policies and procedures, and/or any international, federal or provincial law will be dealt with accordingly. Consequences may include suspension or removal of access to I.T. resources, notification to the Registrar and the appropriate Chair, or the Director of Human Resources as applicable, and/or contact with the appropriate provincial or federal authorities.

POLICY REVIEW:

Due to the ever-changing nature of the information technology environment, this policy will be reviewed regularly by the Corporate Services Office, in conjunction with the Director, I.T., to ensure its relevance and accuracy.

STUDENT CODE OF CONDUCT**PREAMBLE:**

Mohawk College grants the privilege of using information technology resources and facilities (hereafter referred to as I.T. resources) to students, clients, employees and community partners strictly for the purposes of learning, teaching, research, student life, and administration. While the College makes every effort to ensure network security and data integrity, individuals also have certain responsibilities and as such are responsible for making themselves aware of the applicable laws, policies, and guidelines. All students and other academic clients will abide by this *Information Technology Code of Conduct*, the Information Technology Security Policy, and the Information Technology Acceptable Use Guidelines.

GOVERNING STATUTES, REGULATIONS, AND POLICIES:

The use of Mohawk College's information technology resources and facilities is subject to all federal and provincial laws, and to the College's applicable policies and procedures. These include, but are not limited to the following:

Federal

Canadian Bill of Rights
Copyright Act
Criminal [Code](#) of Canada

And others that may be appropriate

Provincial

Freedom of Information & Protection of Privacy Act
Human Rights Code
Libel and Slander Act

And others that may be appropriate

Mohawk College

Information Technology Security Policy (C1020 – previously Computing & Telecommunications Policy)
Information Technology Acceptable Use Guidelines (new)
World Wide Web Page Policy (C125)
Copyright (C140)
Access to Information and Privacy Act (C201)
Use of College Property (C225)
Disruptive Behaviour in the Learning Environment (C229)
Freedom of Information and Protection of Individual Privacy Act Policy (C242)
Threats, Acts of Violence and Weapons Possession (C292)
Access to Student Records (C701)
Academic Dishonesty (C705)
Student Code of Conduct and Discipline (C757)
Human Rights Policy (H320/C202)

SPECIFIC ACTIVITIES:**1. Personal Use:**

Users will **not** use Mohawk College I.T. resources for personal gain or profit, or for political or religious purposes. Resources and facilities must be specifically used for the sole purposes of teaching, learning, research, student life and administration of the College. All equipment, files or programs that reside on a College workstation, server or network are the property of the College.

2. College Access to Electronic Communications and Electronic Files

2.1 Mohawk College cannot guarantee confidentiality of all electronic communications. In order to develop, maintain, or repair the network and its systems, key identified staff members have special access privileges that allow them to gain access to any resources residing on the network. You are therefore cautioned to use discretion when sending or saving electronic communications.

2.2 In accordance with the **Freedom of Information and Protection of Privacy Act**, the public and authorized individuals may have access to a users' electronic records, including electronic communications, stored on College computers, subject to applicable exemption under those Acts.

3. Criminal Offenses:

Users will adhere to all applicable laws of Canada (federal), and Ontario (provincial). For example, the proliferation of pornographic, obscene or abusive materials, or hate literature is forbidden and is punishable by the appropriate authorities.

4. Copyright:

Users will observe copyright and software licensing agreements. For example, copying programs, data, images, audio files, etc. that are the property of another without the owner's expressed authorization, or installing or running unlicensed or illegal software, or allowing the copying, installation or running of unlicensed or illegal programs or files is forbidden and is punishable by the appropriate authorities.

5. Hacking:

5.1 Users will **not** attempt unauthorized access to computer installations inside or outside of Mohawk College using Mohawk College's I.T. resources or facilities.

5.2 Users will **not** forge or misrepresent their identity, or provide false or misleading information to gain access to I.T. resources or facilities inside or outside of Mohawk College.

5.3 Users will **not** deliberately mask the identity of an account or machine.

5.4 Users will **not** probe for loopholes or attempt to circumvent security protection schemes of hardware or software, nor engage in any activity that attempts to compromise the security of any system.

5.5 Users will **not** install or use software or other tools that allow access to others' systems, accounts or passwords.

5.6 Users will **not** tamper with or attempt to tamper with Mohawk College hardware or software settings, or otherwise attempt to break into any other locked down system. For example, users will not attempt to gain access to the Windows Control Panel functions that have been locked out on Open Access and lab computers.

6. Inappropriate Use:

Users will not use Mohawk College I.T. resources to transmit, display, distribute, or make available materials that are harassing or discriminatory, in keeping with the College's Human Rights policy. Illegal, libelous, abusive, obscene, threatening, intimidating or demeaning transmissions to any individual or group are also prohibited. This includes, but is not limited to, the use of electronic mail systems, and postings on electronic bulletin or message boards and web pages.

7. Wasting Information Technology Resources:

Users will **not** waste I.T. resources by playing games, spamming of messages, flooding the network, running or installing programs intended to damage or to place excessive load on a computer or the network (for example, viruses, Trojan horses, worms, etc.), or otherwise interfering with the normal operation of the network, and thus depriving other users of I.T. resources or compromising other users' files or data.

8. User Privacy:

Users will **not** view, destroy, or alter the integrity of any information belonging to another user another without the owner's expressed authorization. All material stored on a server or a computer or transmitted via the network is presumed to be confidential and private. This includes email messages and attached files that may have been sent in error either by the originator or a virus program. Users will not compromise the privacy of any other user by viewing or forwarding such messages or attachments when it is determined that the information was not intended to be distributed.

9. User Accounts and Passwords:

Users will **not** give their accounts or passwords to others, nor allow others to gain access to their accounts or passwords. All accounts and passwords are private and confidential.

10. Reporting Misuse:

Users must report the misuse of Mohawk College I.T. resources to the appropriate Chair, or the Director of Information Technology. Failure to do so may result in the assumption that the user who witnessed the misuse was party to the act.

11. Enforcement and Consequences of Violation:

- 11.1 Violation of federal or provincial laws is enforced and punishable by the appropriate federal or provincial authorities.
- 11.2 Mohawk College policies and codes are the responsibility of the Board of Governors of Mohawk College and are enforced by the appropriate designate. For example, department servers are the responsibility of that department manager. Open Access and general purpose labs are the responsibility of the Director of Information Technology. Enforcement of the policies and codes will be shared by that appropriate individual and the Registrar.
- 11.3 Violation of a Mohawk College policy or this Code of Conduct will result in any **one or a** combination of the following:
 - i. verbal warning(s)
 - ii. written warning(s)
 - iii. restriction or withdrawal of access to resources and facilities
 - iv. suspension from the course or program
 - v. removal from the course or program
 - vi. criminal or civil action

It is the responsibility of all users to familiarize themselves with the Mohawk College Information Technology Acceptable Use Guidelines.

ORIGINATED BY: Director of Information Technology
DATE: June 2002
APPROVED BY: Mohawk College Council
DATE: 2002
REVISIONS: 2002, 2003
Policy Number Change: December 2008

CURRENT REVISION: Director of Information Technology
DATE: February 2003
APPROVAL: President
DATE: March 2003
DISTRIBUTION DATE: June 2003