Policy Number:	**CS-1502-2002**
Policy Title:	**Information Technology – Use and Security**
Policy Owner:	**Chief Information Officer**
Effective Date:	**June 2002**
Last Revised:	**March 2014**

1. PURPOSE

Safe and secure computing practices are essential for maintaining the integrity and security of the College's information and to protect the College, its students and employees.

Mohawk College (herein referred to as the "College") provides computing, information, communication and networking resources and facilities to authorized employees, students and community partners to facilitate teaching, learning, research, student life and administration in support of the College's mission and goals.

This policy sets forth expectations regarding the use by employees and other authorized users of the computing resources and infrastructure owned or managed by the College. The College expects employees to utilize the College computing resources and infrastructure for the conduct of College-related business. Use by students of the College computing resources and infrastructure is subject to the Student Code of Conduct and such other policies as may apply.

2. APPLICATION AND SCOPE

This policy and accompanying procedures have been developed to ensure appropriate use of the College's information technology (IT) resources and facilities and to safeguard the security and integrity of IT networks and data used by employees and other authorized users of the computing resources and infrastructure, specifically;

- 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 IT resources from the 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.

- Implementation of appropriate protection when connecting to the internet in cooperation with existing Internet Service Provider agreements.

This policy applies to all IT resources, stated above, that 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.

3. DEFINITIONS

"Authorized Users" refers to 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.

"Confidential Information" is information regarding any College-related activity not otherwise available to the public which has been created, communicated, or received by or within the College with the expectation that it remain confidential.

"College Computing Resources and Infrastructure" includes but is not limited to: personal computers, workstations, administrative devices, laptops, personal digital assistants (PDAs), wireless connected devices, printers, corporate and academic server systems, software applications (in-house or purchased), operating systems, network devices, internet access, firewalls, electronic storage, email, voicemail, newsgroups, telephone systems, communication peripherals, fax machines, modems, data, transmission of data -electronic data exchange, networks and virtual services owned, operated, managed or licensed by Mohawk College.

"Occasional Incidental and Personal Use" is of minimal time and duration, resulting in no additional cost to the College and does not impact the operations of systems or assigned work.

"Personal Information" (as per Section 2(1) of the Freedom of Information and Protection of Privacy Act (Registered Statutes of Ontario)) (FIPPA) is defined as: recorded information about an identifiable individual, which includes;

(a) information relating to the race, national or ethnic origin, color, religion, age, sex, sexual orientation or marital or family status of the individual,

(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, telephone number, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they relate to another individual,

(f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual and

(h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

"Security" refers to the safety and protection of property from unacceptable risk and/or danger including, but not limited to; tampering, hacking, and/or the spreading of viruses.

4. PRINCIPLES

Since IT resources represent a significant monetary investment by the College, protection of these assets on all levels is paramount. The College recognizes its responsibility, which may be shared with divisions, departments and individuals as appropriate, to ensure the security and integrity of these IT resources, and of all authorized users. Individual users have the responsibility to comply with applicable laws, policies and guidelines.

5. ACCOUNTABILITY AND COMPLIANCE

5.1 Accountability Framework

This policy has been approved by the Senior Management Team.

5.2 Compliance

The Chief Information Officer will monitor and ensure compliance with this policy.

6. RULES

6.1 All individuals using Mohawk College's information technology resources and facilities must comply with:

- Applicable federal and provincial legislation.
- College IT policies and procedures, including the *IT Users' Code of Conduct* as referenced in the Information Technology – Use and Security Procedures.

- Copyright laws and software licensing agreements. Unauthorized or illegal software or hardware must not be installed on any College IT Resources or any computing device connected to the College network.

6.2 Use of IT resources must be responsible, ethical, and lawful at all times. Employees have a duty to ensure that their computer practices do not adversely affect others or expose personal or confidential information to inadvertent disclosure, theft or loss.

6.3 College IT resources must be used for College business, with occasional incidental personal use permitted. The use of College computing resources and infrastructure for personal gain or profit, political or religious use, commercial advertisements, playing games, spamming of messages, broadcasting unsolicited e-mails, including but not limited to the operation of any personal business, or any non-College information is prohibited.

6.4 Internet resources must be used for teaching, learning, research, student life or administrative purposes only. Viewing or listening to material that is illegal, offensive or otherwise inappropriate to the user's function is prohibited.

Downloading of College information must conform to the following;

- Can only download using appropriate authentication
- Can only use data for approved College use
- Cannot pass information to others without permission by appropriate College official

6.5 Notwithstanding that the College permits occasional incidental personal use of its computing resources, information stored within the College's computing infrastructure, including personal information in individual accounts, and e-mail is the property of the College. The College reserves the right to restrict occasional incidental and personal use of computing resources at any time as the College sees fit. The Information Technology Division has the right to check and monitor networking resources and facilities on a regular basis, and reserves the right to take an appropriate action to protect these resources and facilities, in compliance with the Freedom of Information and Protection of Privacy Act (FIPPA). Such monitoring will not be considered a violation of international, federal and provincial laws, FIPPA, or this Policy.

6.6 All authorized users are responsible for the security of the data and files on their computing devices and bear the primary responsibility for the materials being sent, accessed, or displayed. This responsibility applies equally to the use of College computing resources and infrastructure as well as to the use of such innovations as blogs, social networking sites and wikis. Users must respect the public nature of the College, and refrain from sending, posting on electronic bulletin boards, accessing, downloading, disseminating, printing, or displaying any images, sounds, messages, or depictions which could reasonably be expected to be offensive, harassing, or which could reasonably be seen as detrimental to the interests of the College.

6.7 No individual shall knowingly breach, compromise, endanger or threaten the College's IT resources, attempt to do so, or allow others to do so. Users must report misuse of college IT resources to the appropriate Manager, or the Chief information Officer. Failure to report misuse may result in the assumption that the user who witnessed the misuse was a party to the act.

6.8 Any user who does not comply with the provisions of this policy and/or an international, federal or provincial legislation will be subject to sanctions. Violation of federal or provincial laws is punishable by the appropriate federal or provincial

authorities. Non-compliance with college IT policies and procedures will result in any one or a combination of the following penalties;

i) verbal warning(s)
ii) written warnings
iii) restricted access or complete withdrawal of access to IT resources
iv) suspension from the course or program
v) removal from the course or program
vi) criminal or civil action.
vii) dismissal or termination with cause
viii) cost recovery

6.9 The College reserves the right to issue or deny user access to any College IT resource, as considered appropriate. The Chief Information Officer, together with the Registrar or Chief Human Resources Officer has the authority to limit access to College IT resources.

- Terminated or retired employees do not have access to College IT resources except as specifically approved by the CIO (or other authorized College Official). Access to files, including any personal files on the employee's workstation or network server will cease on the last day of work. This does not include personal information.
- Students whose relationship with the College has been terminated through suspension or expulsion do not have access to College IT resources.

6.10 Anyone with a computing device which uses IT resources will be required to formally acknowledge these policy guidelines. Acknowledgement of these policy guidelines shall occur either electronically or by signature.

7. POLICY REVISION DATE

7.1 Revision Date
February 2017

7.2 Responsibility
The Chief Information Officer is responsible for monitoring this policy every three years or more frequently in response to feedback from the College community.

8. ATTACHMENTS
Appendix A- Information Technology- Use and Security Procedure
Attachment 1- Information Technology Users' Code of Conduct
Attachment 2 - Information Technology - Hardware Registration Form

9. SPECIFIC LINKS
SS-3200-2006 Student Behaviour Policy
CS-1502-2002 Information Technology Use & Security Policy
CS-1501-2007 Electronic Communications Policy
CS-1306-1979 Conflict of Interest

CS-1503-2007 Wireless and Cellular Technology
C125 - World Wide Web Page Policy
GC 4200–2013 Social Media Policy
GC-4101-2013 Copyright Policy
Employee Code of Conduct
CS-1008-2014 - Acceptance of Payment Cards (under development)
Freedom of Information and Protection of Privacy Act

Appendix A
Information Technology - Use and Security Procedure

P1. Roles and Responsibilities

P1.1 Chief Information Officer

The Chief Information Officer 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;
- College IT resources
- The telecommunication systems, including e-mail; collaboration tools, social networking, telephone, wireless devices and voice mail systems.

P1.2 Departments and Information Custodians

- Department Managers (Deans, Associate Deans, Directors, and Managers) 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 Policy and the User Code of Conduct, and for ensuring that access to resources is removed upon termination of employees suspension or expulsion of students.
- Department managers are responsible for maintaining their own licensing agreements, having all appropriate licensing documentation, for any software acquired through the department, and complying with college copyright policies and procedures. The Information Technology division assumes responsibility for college-wide licenses.
- The Chief Human Resources and Organizational Development Officer are responsible for the Human Resources Information System, the Registrar for the Student Information System, and the Vice President, Corporate Services for the Finance System.
- The Chief Building & Facilities Officer is responsible for the physical security of all resources and facilities.

P1.3 Individual Users

- All authorized users are responsible for the security of the data and files on computing devices.
- Private student information or information otherwise considered confidential shall not be stored on cloud services such as Google Drive or Dropbox.
- Complete the appropriate paperwork required when borrowing/loaning out equipment from the IT Service Desk.

P2. Procedures for Using Personal Computer Devices and Network Resources

P2.1 Take appropriate steps to protect your computer, software and files. 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.

Create a password that is meaningful and easy to remember, but difficult for others to guess. The password should be a minimum of seven characters with numbers as well as letters. The use of proper names or a dictionary word is not recommended since these are easy for hackers to decipher. It is recommended that you change your password every 3 months. You are required to use the MoCoMotion Secret Questions and Answers Setup and follow the password requirements" found under "My Account Preferences" once you logon to MoCoMotion. If you suspect a hacking attempt or infiltration change your password immediately. Use a different password for each system.

Be diligent in performing routine backups to guard against the loss of information.

P2.2 Register for the self-service password reset functionality available on MoCoMotion.

P2.3 Keep your accounts and passwords confidential. Use of someone else's account or password, or forging an account or password is prohibited.

P2.4 PDAs, Blackberries, and other wireless-connected devices used to access College computing resources and infrastructure must have password protection enabled.

P2.5 Lost or compromised passwords must be reported to the helpdesk immediately.

P2.6 Employees are required to report the loss or theft of College computers, PDAs, Blackberries, etc. to their supervisors, campus security services and local authorities where appropriate as soon as possible.

P2.7 Employees are required to notify their superiors in the event of any known or suspected breach of security, loss of information, or introduction of a virus or malware into the College's computing infrastructure or network.

P2.8 Ensure that the necessary virus protection software is installed with the most current virus definition file to scan all software and files received from others or downloaded from the internet to avoid damaging or overloading the computer system or network.

If you believe that you have received a virus in an email message, do not open it. Contact the IT Service Desk or the IT Division immediately.

P2.9 Encrypt sensitive or confidential information before transmitting it via the internet. Data stored on USB keys and computing devices must be encrypted. When viewing sensitive data over the internet you must ensure that you are using a secure connection. Eg. HTTPS"

P2.10 If you are working within a transactional web based application (eg. CE Registration) do not copy URL's that contain session security and distribute to others via email or other methods. Transactional web applications usually involve the input or processing of personal or financial information.
Eg. URL's that contain a security or session token

P2.11 Get approval from the IT Division if you require your own personal computer devices or personal networking equipment (including interfaces and software) to be connected to your workstation or to the College network. Before any equipment is installed, you must complete Attachment 2, Information Technology Hardware Registration Form, and submit it to the IT Division with approval from your manager.

P2.12 Contact the IT Helpdesk, manager approval required, to have the applicable system administrator to provide or remove access to a particular system and/or information. Accounts and passwords are managed by those administrators only and access cannot be granted by unauthorized individuals.

Managers are responsible to inform system administrators via the IT HelpDesk when staff members have left a department to ensure changes in access requirements are managed accordingly.

P2.13 Remove or make arrangements to retain all personal data and files before leaving the College, whether upon completion of a semester or termination of employment. The College will remove access to all Mohawk College IT resources upon termination of employment or study at the College.

P2.14 Refer to CS-1501-2007 Electronic Communications for procedures relating to the use of:
Voice Communications
Voice Mail Broadcast Messages
E-Mail
MoCoMotion Announcements
Creating, Maintaining and Monitoring Groups within MoCoMotion
Creating and Maintaining Channels within MoCoMotion

P2.15 Refer to CS-1503-2007 Wireless and Cellular for policy statements and procedures related to wireless equipment owned by the College.

ATTACHMENT 1
Information Technology Users' Code of Conduct

1. **Personal Use:** Mohawk College IT resources are to be used solely for the 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.

   Users must not waste IT resources by playing games, spamming messages, flooding the network, running or installing programs intended to damage or place excessive load on a computer or the network (e.g. viruses, Trojan horses, worms, etc.) or otherwise interfering with the normal operation of the network and thus depriving other users of IT resources. If the user receives such activity – email containing a virus, then he/she must contact the IT Service Desk or IT Division immediately to avoid threatening or compromising the security of the Colleges systems or networks.

2. **Compliance with Legislation**: Users must adhere to all applicable federal and provincial legislation.

3. **Copyright:** Users must comply with copyright, patents, intellectual property laws, contractual obligations, and software licensing agreements. For example, copying programs, data, images, audio files, etc. that are the property of another, without the expressed authorization of the owner, or installing or running unlicensed or illegal software, or allowing the copying, installation or running of unlicensed or illegal programs or files is forbidden. Violations are punishable by the appropriate authorities.

4. **Hacking:**
   - 4.1 Users must not attempt unauthorized access to computer installations inside or outside of Mohawk College using the college's IT resources.
   - 4.2 Users must not forge or misrepresent their identity, or provide false or misleading information to gain access to IT resources inside or outside of Mohawk College.
   - 4.3 Users must not deliberately mask the identity of an account or machine.
   - 4.4 Users must not probe for vulnerabilities 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.
   - 4.5 Users must not install or use software or other tools that allow access to the systems, accounts or passwords of others.

5. **Human Rights Compliance:** Users must not use college IT 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 or intimidating or demeaning transmissions to any individual or group are prohibited. This includes, but is not limited to the use of electronic mail systems and postings on electronic bulleting or message boards or web pages.

6. **User Privacy:** Users must 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 attachments that may have been sent in error, either by the originator or a virus program. Users must 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.

7. **User Accounts and Passwords:** Users must not distribute their account credentials to others and must make every reasonable effort to safeguard their credentials."

8. **Reporting Misuse:** Users must report the misuse of Mohawk College IT resources to the appropriate Associate Dean, or the Chief Information Officer. Failure to do so may result in the assumption that the person who witnessed the misuse was party to the act.

Attachment 2
Information Technology - Hardware Registration Form

Please Print

Requestor's Name: _____ Date: _____

Requestor's Signature: _____

Phone #: _____ Room #: _____ Campus: _____

Email: _____

Department: _____

It is the responsibility of the person above to ensure this device does not cause any disruptive behaviour on the College network. The device will be banned from the network for any disruptive behaviour.

Device Description: _____

Reason for Device: _____

Make: _____ Model: _____ S/N: _____

MAC Address: _____

Installed Location: _____ (Room including Campus)

If Location is Roaming – Please Describe: _____

Duration of Use: _____

College Manager or Sponsor: _____ Phone #: _____

Email: _____

Sponsor Signature: _____ Date: _____

To be completed by IT Division

IP Address: _____ Switch/Port: _____

Comments: _____

_____

Approval Signature: _____ Date: _____