1. Purpose
The purpose of this policy is to provide College employees with guidance on acceptable and unacceptable use of the College’s Information Technology (IT) resources. In addition, this policy supports effective organizational security and protects users and IT resources from but not limited to cyber criminals, bullying, misuse of accounts and assets, and the spread of malicious software.

2. Application and Scope
This policy applies to all employees, contractors, consultants, volunteers or other workers including College community members that use any component of the College’s IT resources regardless of the physical location or device used. This policy excludes students, except where students are employed by, or on a work placement with, the College.

3. Definitions

“Authenticate” refers to the process of logging onto an IT resource by validating a user’s identity. This is typically completed by providing a username and then validating that username by providing something you know such as a password, something you have such as a card, or by providing something you are – such as a biometric piece of information (fingerprint, retina scan, palm, etc.).

“IT Infrastructure” refers to software, hardware, devices, networks, server systems, data storage, data centres, related equipment, and cloud-based technologies.

“IT resources” refers to any IT Infrastructure component that can be interacted with and used by individuals such as a computer, application, mobile phone, data, etc.

“Manager” refers to a person who has charge over a workplace or authority over a worker, including, Managers, Directors, Associate Deans, Deans, Registrar, Chiefs, Vice Presidents and President.

“Sensitive Information” includes information that should not be shared and may include restricted, confidential, or personally identifiable information or documents which may be marked as “Internal Use Only.”

“User(s)” includes any person that uses or operates an IT resource.
“VPN” stands for Virtual Private Network and is a software application that creates a secure encrypted tunnel between a remote computer and the College campus. Using this technology ensures that data communications are kept secure.

4. Principles
This policy is based on five key principles:

A. Ethics, Values and Fairness
Exercise common decency, good judgement, and respect for the College community members and property.

B. Security
Preserve the integrity and availability of systems and services and ensuring that actions taken by College community members do not negatively affect College IT resources.

C. Privacy
Protect and safeguard College IT infrastructure and information.

D. Compliance
Use of IT resources adheres to all legal, regulatory and College policy requirements.

E. Productivity
Access to IT resources is uninterrupted and accessible when needed.

5. Accountability and Compliance

5.1 Accountability Framework
This policy has been approved by the Senior Leadership Team.

5.2 Compliance
The Chief Information Officer, in cooperation with other departments, will monitor and ensure compliance with this policy.

6. Roles and Responsibilities

6.1 Chief Information Officer
The Chief Information Officer is responsible for the security of all IT resources.

6.2 Managers
Managers are responsible for:

- communicating IT security policies and procedures to employees;
- complying with all IT policies and procedures;
- ensuring that IT resources are procured with IT’s approvals and configured and maintained in compliance with all IT Standards.
- the security of IT resources managed by their department;
- authorizing access to systems and information;
• ensuring completion of any mandatory IT training; and
• requesting removal of access rights to the IT Service Desk at the end of, or change of, employment including all employees, contractors, or consultants.

6.3 Individual Users of IT Resources
All users of IT resources are responsible for protecting the confidentiality, integrity, and availability of our information and systems in accordance with this policy.

7. Rules

7.1 Authorized Use
All individuals using Mohawk College IT resources must use those resources to carry out the functions for which they were authorized, specifically:

• Access to IT resources shall only be provided to active employees, contractors, consultants, temporary, part-time, or other workers. Visitors may be provided access to limited resources pending approval and registration with the IT Service Desk.
• Use of IT resources must align with the appropriate Academic, Support or Administrative intentions for which they are provided.
• Access to and use of IT resources is limited to those which the employee is authorized to use.
• Employees must always authenticate using the College provided account which was assigned specifically to them to access IT resources and should not use any other user account other than their own when accessing IT resources.
• Employees must return all IT resources at the end of employment or when their role changes including but not limited to desktops, laptops, portable media, and cell phones.

7.2 Personal Use

7.2.1 Occasional personal use of IT resources is permitted in accordance with the following. Users:

• Must not use IT resources in a way that interferes with employment duties.
• Must not create any monetary cost to the College.
• Must keep browsing limited to trusted, reputable websites.
• Must not threaten the security or availability of IT resources.
• Personal files stored on IT resources will not be accessible or returned at the end of employment.

7.2.2 Although the College permits occasional personal use of its IT resources, the College reserves the right to restrict occasional incidental personal use of IT resources at any time and as the College sees fit.

7.3 Prohibited Use
All individuals using Mohawk College IT resources are strictly prohibited from:
• Using IT resources for any political, religious, or commercial activity, or, for conducting any personal business in which they would receive personal or financial gain unless they have received permission from the College in writing, and in accordance with the Conflict of Interest Policy.
• Using IT resources in a way that interferes with employment duties, or, creates any monetary cost to the College.
• Exporting software from the College for resale or distribution.
• Accessing or creating discriminatory, defamatory, bullying, harassing, offensive, pornographic, or obscene content.

7.4 Security

7.4.1 Users of IT resources must not knowingly place the security of information or systems at risk. At all times, Users must:

• Ensure that IT infrastructure and resources are configured and maintained in accordance with all IT Standards.
• Never disclose any component of sensitive information unless the recipient owns, or is authorized to have access to the information.
• Contact the IT Service Desk immediately in the event of an IT security incident, see Appendix A for procedure.
• Keep secret authentication information such as passwords, pin codes, or any other authentication information secure and at no time share authentication information with any individual.
• Take precaution prior to opening any attachment or clicking on links within electronic messages.
• Store all work on central College servers to ensure that sensitive, confidential and personal information is protected and that work is backed up regularly.
• Never use personal e-mail accounts to conduct College business.
• Only use cloud services which are approved by IT and have been subject to a cloud or third party risk assessment by IT Security.
• Never upload sensitive, confidential or personal information to cloud or third party sites without approval from IT Security.
• Never install untrusted software or applications on IT infrastructure or resources.
• Always use the College provided VPN when performing work remotely.
• Ensure that personally owned devices that may come in contact with IT resources are protected with antivirus software, a personal firewall, and regularly install security updates and patches to operating systems, applications, and web browsers.

7.4.2 No individual shall knowingly breach, compromise, endanger or threaten the College’s IT resources, attempt to do so, or allow others to do so. This includes probing, scanning, assessing, penetrating or affecting the availability of College IT resources. Users must report any misuse of IT resources to the IT Service Desk, or to the Chief Information Officer. Failure to report misuse may result in the assumption that the User who witnessed the misuse was party to the act.
7.4.3 Mohawk College reserves the right and responsibility to protect the College and community members from inappropriate use of IT infrastructure and resources by taking actions, including but not limited to:

- Monitoring systems, networks, services, accounts, and web activity.
- Providing access to only current active employees, contractors, consultants, other workers, further:
  - Termination of employment will disable access to all College IT resources and all IT assets must be returned.
- Denying a user the right to access IT resources at any time the College deems necessary.

7.5 Compliance
Use of the College’s IT resources is subject to, and must comply with, all applicable laws and College policies and procedures, including this policy. Non-compliance with applicable laws and regulations may result in civil liability or criminal prosecution. The College reserves the right to restrict or deny access to its IT resources, to monitor your use of those resources and to take actions it deems necessary or appropriate to protect College IT resources. By using the College’s IT resources, Users are confirming agreement with this policy.

In addition to the above, Users of IT resources must also comply with:

- Applicable collective agreements, terms and conditions of employment and code of conduct;
- Copyright Laws including, but not limited to, the sharing of pirated software, audio, and video.
- Licensing agreements; and
- Any other agreements between the College and an external service provider.

7.6 Noncompliance
Noncompliance with this policy may result in any one or combination of the following sanctions:

- Verbal warnings;
- Written warnings;
- Restricted access to, or complete withdrawal of access to IT resources;
- Suspension from work;
- Termination;
- Recovery of costs due to damages or fees; and/or
- Criminal or civil action.

8. Policy Revision Date

8.1 Revision Date
September 2020
8.2 Responsibility
The Chief Information Officer will review this policy every three years or earlier where required.

9. Attachments
Appendix A - Reporting an IT Security Incident

10. Specific Links
CS-1306-1979 Conflict of Interest Policy
CS-1317-2012 Respectful Workplace (Harassment and Discrimination) Policy
CS-1500-2013 Web Posting and Electronic Notifications Policy
CS-1501-2007 Electronic Communications Policy
CS-1503-2007 Wireless and Cellular Technology Policy
GC-4100-2013 Intellectual Property Policy
GC-4101-2013 Copyright Policy
GC-4200-2013 Social Media Policy
Academic Collective Agreement
Support Staff Collective Agreement
Terms and Conditions of Employment for Administrative Staff
Mohawk College Strategic Plan
Employee Code of Conduct
Privacy and Legal Statements
Copyright Act
Employee Departure Checklist

IT Standards – Available upon request
Appendix A
Reporting an IT Security Incident

What is an IT Security Incident?
An IT is an incident that may affect the confidentiality, integrity or availability of the College’s IT infrastructure through unauthorized access, accidental disclosure, or other, including:

- The presence of any form of malicious software (malware, viruses, worms, etc.).
- The presence of any abnormal software that was not previous present on a computer or server.
- Suspicion that your user account has been compromised.
- Intentional or accidental exposure of sensitive information.
- Web browsers re-directing automatically or producing popup messages or advertisements unexpectedly.
- File types, formats, or naming conventions changing unexpectedly or files not opening as expected.
- Slow computer performance, applications hanging, or any unexpected behaviour.
- Notifications that anti-virus or firewalls are not running or are disabled.
- Lost or stolen devices including but not limited to laptops, mobile phones, desktop computers, portable storage devices, switches, etc.

Reporting an IT Security Incident

1. Disconnect the network cable from the computer.
2. Do not power off the computer.
3. **Contact the Mohawk College IT Service Desk immediately** by phone if you believe you are experiencing an IT Security incident regardless of your location.
   - Phone: 905 575 1212 x2199
   - E-mail: helpdesk@mohawkcollege.ca
4. Inform your immediate manager of the current status.
5. Make notes about the IT incident to make sure that you can provide clear and accurate information to IT staff.
   - When making notes, consider the following:
     i. What happened?
       1. What websites have I visited recently?
       2. Have I received any suspicious e-mails that were actioned recently?
     ii. When did it happen? (specifically at what time)
     iii. Where did it happen (Physical Location and Network Location (ex: Wireless))?
     iv. Who was involved?
     v. Could there be sensitive, personal or confidential information at risk?