1. Purpose

The purpose of this document is to provide instructions on researching, selecting, implementing, and maintaining IoT (Internet of Things) and OT (Operational Technology) devices. This document applies to all employees, students, researchers, third parties, partners, or contractors at any Mohawk College location or sanctioned event.

IoT or Internet of Things is a network of connected devices that interact and exchange information with each other. The technology allows connection of two or more devices that connect with each other and send and receive information through a network. These devices usually do not require direct human interaction with a computer to function. Examples may be, but not limited to, lighting fixtures, person sensors, thermostats, vibration sensors, flow meters, water sensors, tracking devices, weather stations, or video/security camera’s.

OT or Operational Technology is IoT systems applied to direct monitoring or controlling of physical assets that operate the College. An example may be HVAC systems, lighting systems, CCTV camera’s, among others.

2. Guidelines

2.1 Before Implementation, Testing, or Procurement

- Research devices before you purchase:
  - Read reviews.
  - Get recommendations from partners.
  - Research their security capabilities.
  - Ask the vendor how they meet security requirements from this document.
- Ensure that devices integrating with Cloud services have been assessed using the Third Party
Security Assessment Questionnaire available from IT Security via contacting the Helpdesk.

- Ensure devices have a system reset capability to set them back to factory default.
- Identify points of contacts with the manufacturers for any future issues.
  - Identify if the vendor maintains devices and if patches are available.
  - Understand and plan around the end of life, or end of support for the product. Consider what funds you will require to replace and refresh the devices and when you will require the operating funds to do so.
- Read device materials, operator’s manuals, instructions, and support forums.
- Plan to have a support contract in place for OT (Operational Technology).
- Plan to maintain an asset inventory of your devices. Information you should capture includes:
  - Device Manufacturer
  - Device Model
  - Deployed Location
  - IP Address
  - MAC Address
  - Description
  - Department
  - Device Owner

2.2 During implementation:

- Default passwords on all devices must be changed.
  - Use strong passwords in compliance with IT Password Policies (Appendix A).
  - Set unique passwords for Mohawk College.
    - Passwords should never be the same as other organizations.
- Document the devices in an asset inventory and store for audit purposes.
  - Ensure that asset inventory can be easily produced upon request.
- For hardware deployed in public places ensure that the hardware is tamper and theft proof, casing and mounting options should be considered. If USB or other ports are accessible, ensure that casing protects them so unauthorized individuals cannot use them.
- If your device supports logging, work with IT Security to get the logs into a centralized tool via a Helpdesk ticket.
- Where possible, set operating system, software, and firmware to update automatically. Establish periodic manual updates as required.
- If the operating system permits, install the latest antivirus and antimalware capabilities on each device operating system.

Network requirements during implementation:

- Ensure that IT is consulted with and configures network ports for the device. The network should be segmented behind a firewall and not on the campus public network.
- Traffic from the devices should be encrypted where possible, work with your vendor. Encryption protects information, but also ensures integrity of the messages sent. Where possible:
  - Use the latest versions of TLS.
  - Use up to date cryptographic functions.

2.3 After implementation

- Ensure devices remain up to date.
- Keep an accurate inventory of the devices
• Update asset inventories when devices are added, modified, or removed.
• Monitoring of systems should be conducted as business as usual activity.
• Report any lost or stolen devices to IT Security.

3. Additional Considerations

Consider the following when selecting and deploying IoT or OT technologies. This will help you understand the risks and deployment considerations you may need to make:

What do the IoT devices or systems need to access or communicate with?
  o Do they physically control something? (Lights, Heating/Cooling, Doors)
    ▪ Does their output contribute to controlling something?
  o Do the IoT devices or systems need access to internal network resources, if so which resources?
  o Do the IoT devices or systems require inbound access from the Internet?
  o Do the IoT devices or systems require outbound access to the Internet?
  o Do service providers of these devices or systems require remote access from the internet?
    ▪ If so, ensure you work with IT to register your vendor’s access.
  o Do these devices communicate to a SaaS (Software as a Service) Cloud Solution or internal web server?

4. Failure to Follow Guidelines

Failure to follow these guidelines during implementation will be dealt with under the applicable acceptable use policies.
Appendix A

Password Requirements

Users must select passwords of high quality and Information system administrators must provision access control systems to enforce the following as closely as possible.

Passwords Must:

- Be at least eight characters in length
- Not be the same as the last four passwords used
- Be free of multiple consecutive characters or numbers (e.g. ‘aaaa’, ‘abcd’, ‘1111’, ‘1234’)
- Be easy to remember
- Not contained in Mohawk College’s Password Blacklist
  - Any of the follow words regardless of case or characters:
    - Mohawk
    - College
    - Student
    - Campus
    - Fennell
    - Stoney
    - Creek
    - IAHS
    - change
- Not have previous breach exposure
  - Check this site: https://haveibeenpwned.com/Passwords
- Not be based on anything that someone could easily guess.
- Not be a singular dictionary word.
- Not be used for both business and personal usage.
- Must be changed at first logon if temporary.

For questions on this password policy, please contact the Helpdesk at 905 575 2199.