Classification Number	*To be assigned by Policy Office*
Framework Category	Administrative
Approving Authority	*To be assigned by Policy Office*
Policy Owner	
Approval Date	DRAFT FOR CONSULTATION
Review Date	
Supersedes	

ELECTRONIC MONITORING POLICY

PURPOSE

1. The Ontario Working for Workers Act, 2022 requires certain employers to introduce a written policy regarding its electronic monitoring practices. To that end the purpose of the Electronic Monitoring Policy ("the Policy") is to provide information and transparency about how the University may electronically monitor and collect information pertaining to its employees.

DEFINITIONS

2. For the purposes of this Policy the following definitions apply:

"Active Electronic Monitoring" means the use of devices or software to intentionally track the activities and/or physical location of an identified employee or employees.

"Passive Electronic Monitoring" means the routine collection, analysis, and retention of information or activity in physical spaces and on the digital network.

SCOPE AND AUTHORITY

3. This Policy applies to all employees of Ontario Tech University (" University"). For clarity, "employee" under this Policy means only those employees of the University who are considered employees as defined by the Ontario Employment Standards Act, 2000 ("ESA").

4. This Policy does not provide employees any new rights or right to not be electronically monitored. Nothing in this Policy affects or limits the University's ability to conduct electronic monitoring, or use information obtained through electronic monitoring.

5. Nothing in this Policy is intended to amend or supersede any grievance procedure or other aspect of any applicable collective agreement.

6. The Chief Transformation and Organization Culture Officer, or the successor thereof, is the Policy Owner and is responsible for overseeing the implementation, administration and interpretation of this Policy.

POLICY

7. For purposes of this Policy, the University has distinguished any applicable monitoring as either Active or Passive Electronic Monitoring.

8. **Active Electronic Monitoring**

8.1. The University does not, as a normal course of business, engage in Active Electronic Monitoring for the purpose of employee performance management.

8.2. Active Electronic Monitoring of employees may be undertaken in accordance with the University's Technology Use Policy.

8.3. Examples of Active Electronic Monitoring of employees include, but are not limited to:

a) Monitoring—by video surveillance or otherwise-- the date and time of access to physical locations and digital resources.

b) Monitoring internet resource requests.

c) Monitoring physical location using global positioning system (GPS) technology.

8.4. Active Electronic Monitoring of employees may also include direct access to the contents of the personally assigned account(s) and/or the device(s) used by an identified employee, which may include, but are not limited to, email, voicemail, SharePoint, OneDrive, Google Drive and other storage space assigned for use by an individual employee.

9. Passive Electronic Monitoring

9.1. The University reserves the right to use data that has been collected and retained from Passive Electronic Monitoring and may access information from the personally assigned account(s) and/or devices(s) of an identified employee including for purposes outlined in the University's Technology Use Policy.

9.2. The University has reserved, but is not limited to, the following rights:

a) To collect data relating to activities on University premises and on the university network that may be attributable to identifiable persons.

b) To use the data for the purpose of assuring safety, security, and comfort within physical spaces on University premises, and other uses deemed appropriate and necessary.

c) To use the data for the purpose of assuring the availability, integrity, and confidentiality of digital assets and resources connected to the University network or otherwise provided by the University, and for other uses deemed appropriate and necessary.

9.3. When an employee retains information related to University business operations or the operation of their department, unit, or team within their personally assigned account(s) and/or devices, and that employee is not available to retrieve the information, the University may directly access the account of the employee with oversight from appropriate authorities and in compliance with relevant legislation and University policies.

9.4. In the event that the University collects any personal information, as defined in the Freedom of Information and Protection of Privacy Act ("FIPPA") when using the electronic monitoring tools listed in Appendix A, the University shall collect, use and

disclose personal information in accordance with the applicable legislation, including, but not limited to, FIPPA.

10. Posting, Notice and Retention

10.1. The University will provide all current employees with access to or a copy of this Policy within 30 calendar days of implementation. The University will provide all employees hired after this Policy is implemented with access to or a copy of this Policy (or the applicable revised version) within 30 calendar days of the employee's start date. The University will provide a copy of the Policy to all assignment employees assigned to perform work for the University within 24 hours of the start of the assignment or within 30 days of its implementation, whichever is later.

10.2. The University will retain a copy of this Policy and any revised version of this Policy for a period of three (3) years after it ceases to be in effect.

11. Amendments

11.1. This Policy may be amended from time to time in the University's sole discretion, in accordance with the University's Policy Framework, in which event it will provide an amended copy of the Policy to all employees within 30 days of the date the amendment becomes effective.

MONITORING AND REVIEW

12. This Policy will be reviewed as necessary and at least every three years. The, Chief Transformation and Organization Culture Officer, or successor thereof, is responsible to monitor and review this Policy.

RELEVANT LEGISLATION

13. Ontario Working for Workers Act, 2022, S.O. 2021, c. 7 – Bill 88

Ontario Employment Standards Act, 2000, S.O. 2000, c. 41

Ontario Occupational Health and Safety Act, R.S.O. 1990, c. O.1

RELATED POLICIES, PROCEDURES & DOCUMENTS

14. Technology Use Policy

Personal Use of University Resources

Ethical Conduct Policy

Appendix: Examples of current specific uses of passive electronic monitoring data (which may be changed or updated from time to time)

Passive Electronic Monitoring of physical spaces
The University collects data and information about activities in physical spaces on the university premises. This data includes, but is not limited to, video, audio, physical access requests through electronic door locks, and the physical location of devices on university premises.

Security Cameras
Security cameras collect and retain video of physical spaces. Security camera locations are selected at the discretion of the University.

Electronic Door Locks
Electronic door locks collect and retain logs of physical access attempts to restricted areas. Data collected may include, and is not limited to:

- the date and time of the request,
- the unique identifier of the card being used to attempt access.

Passive Electronic Monitoring of digital identities, assets, and resources
The University collects data about network requests made by devices on the wired and wireless network. This data may include, and is not limited to, the date and time of the request, the name and internet protocol address ("IP address") of the requesting device, and the name and IP address of the digital asset or resource being requested, and the physical location of the requesting device.

The University collects data about cybersecurity threats within the content of network sessions. This data may include, and is not limited to, the results of malware scans, and the behaviour of executables, files, software, code, and processes when opened or accessed, and other data about cybersecurity threats.

Domain Name System (DNS) Servers
DNS servers collect and retain logs of internet resource requests. Automated analysis of internet resource requests is performed to prevent exposure to known cybersecurity threats. Data collected and retained may include, and is not limited to:

- the date and time of the request,
- the name and IP address and the requesting device,
- the name and IP address of the resource being requested (e.g., websites and other resources that are accessed by devices on the university network),
- details about cybersecurity threats prevented and/or detected.

Data collected by DNS Servers may be correlated with other data sets to monitor activities of an identifiable person or persons.

Firewalls

Firewalls collect and retain logs of network connections, including connections from the internet to digital assets and resources on the network, connections from devices on the network to websites and other resources on the internet, and connections between devices on the network. Automated analysis of network connections and the content thereof is performed to prevent exposure to known cybersecurity threats. Data collected may include, and is not limited to:

- the date and time of the request,
- the name and IP address and the requesting device,
- the name and IP address of the resource being requested (e.g., websites and other resources that are accessed by devices on the university network).
- details about cybersecurity threats prevented and/or detected.

Data collected by Firewalls may be correlated with other data sets to monitor activities of an identifiable person or persons.

Authentication and Authorization
The University collects data about authentication attempts to digital assets and resources. This data may include, and is not limited to, the date and time of the authentication attempt, the authentication identifier (e.g., network ID) and IP address of the requestor.

Azure Active Directory
Digital assets and resources collect data about successful and unsuccessful authentication attempts.

Active Directory

Digital assets and resources collect data about successful and unsuccessful authentication attempts.

ADFS- Active Directory Federation Services

Digital assets and resources collect data about successful and unsuccessful authentication attempts.

The University collects data about communications entering, leaving, and within the network. This data includes, but is not limited to, the date and time of the communication, identifiers of the sender and recipient, names and IP address of devices that have handled messages, subject, details about the size and type of attachments.

The University collects data about cybersecurity threats within the content of attachments to communications. This data may include, and is not limited to, the results of malware scans, and the behaviour of executables, files, software, code, and processes when opened or accessed, and other data about cybersecurity threats.

Microsoft365

The Microsoft365 platform retains logs of text, video, and audio communications on the Teams application.

Email
Email servers, including Microsoft Exchange Online, retain logs of email communications.

Email servers, including Microsoft Exchange Online, retain logs of the results of cybersecurity threat analysis on the content of messages. Content may be retained if a cybersecurity threat is detected or suspected.

Audit and Compliance
The University collects data about access to and use of university records and other high value files. This data includes, but is not limited to, the date and time of the access, the authenticated person's identifier (e.g., network ID), actions taken on the record or file (e.g., create, modify, delete, download, etc.).

Microsoft SharePoint
Applications and sites on the Microsoft SharePoint platform may be configured to retain activity and audit logs.

Banner

Banner applications and sites may be configured to retain activity logs.

Fast

Applications and sites on the Fast platform may be configured to retain activity and audit logs.

Canvas

Applications and sites on the Canvas platform may be configured to retain activity and audit logs.

My Ontario Tech

Applications and sites on the My Ontario Tech platform may be configured to retain activity and audit logs.

Endpoint Management and Protection
The University collects data about cybersecurity threats on university owned and issued devices, and personally owned devices that are protected by endpoint protection software managed by the University. This data includes, but is not limited to, the results of malware scans, internet

resources to which the device has connected, and the behaviour of executables, files, software, code, and processes when opened or accessed, and other data about cybersecurity threats.

Microsoft System Center Configuration Manager (SCCM)

Microsoft SCCM collects and retains activity and audit logs.

Microsoft Defender

Endpoint protection software collects logs of cybersecurity threat analysis on the content of files and network connections. Content may be retained if a cybersecurity threat is detected or suspected.