POLICY

ELECTRONIC MONITORING POLICY

Approval Authority: Executive Group

Established On: 2022/09/22

Amendments: N/A

Category: Administrative

1.0 POLICY STATEMENT

The purpose of the Electronic Monitoring Policy is to provide information and transparency about how the NOSM University may electronically monitor and collect information pertaining to its employees.

This policy describes the circumstances in which employees are electronically monitored and is developed in accordance with the *Employment Standards Act, 2000 (ESA)* amendments included in *Bill 88, the Working for Workers Act, 2022*.

2.0 SCOPE

This policy is applicable to all employees of NOSM 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").

This policy does not supersede OPSEU Local 677 Local #1 or #2 collective agreements

This policy excludes the monitoring of financial transitions and other controls that are required for compliance such as the monitoring of corporate card purchases or point-of-sales systems.

3.0 DEFINITIONS

3.1 "Active electronic monitoring" is the use of devices or software to intentionally track the activities and/or physical location of an identified employee or employees.

3.2 "Passive electronic monitoring" is the routine collection, analysis, and retention of information or activity in physical spaces or via the computer network.

3.3 "Electronic monitoring" is the collection and/or use of information about an employee by means of electronic equipment, software (including those managed or hosted by a third-party, e.g., cloud-based software) or the University computer network.

3.4 "Record" is any information stored by the employer that contains identifiable information about an individual in relation to an activity or event such as a system access action or file deletion action.

4.0 POLICY TERMS

4.1 Privacy

4.1.1 The employer does not engage in active electronic monitoring for the purpose of employee performance management.

4.1.2 The employer may use active electronic monitoring data for the purposes of investigating physical security events, cybersecurity incidents, or in cases of suspected criminal activity in accordance with municipal, provincial, or federal laws.

4.1.3 Records may be provided to third parties as part of a Freedom of Information of Information and Protection of Privacy Act (FIPPA) request with the exception of teaching materials or data not in the possession of NOSM University.

4.2 Data retention

4.2.1 Retention schedules vary by system and are maintained in accordance with legislative or FIPPA regulations.

4.3 Monitoring circumstances, purposes, and types:

System	Circumstances and purpose of monitoring	Type (Datatype)
Building access control system	The property owners maintain building access records for security auditing or incident response purposes.	Passive (Logs)
Email and chat	Intended for incident investigation, capacity planning, and backup purposes. Message contents are not monitored.	Passive (Logs)
Learner safety app	Some safety features require location tracking which can only be enabled by the employee on their mobile device.	Active (GPS location)
Network Traffic	Intended for bandwidth allocation and incident investigation purposes.	Passive (Logs)
Network printers and photocopiers	Unit-based copy codes are used to identify usage trends.	Passive (Logs)
Security cameras	The property owners have installed campus security cameras in common areas for security purposes.	Active (Live feed and recordings)
System access	All NOSM U IT systems log system access. Some systems also gather general geolocation data based on IP address for cybersecurity purposes.	Passive (Logs)
Telephone & fax system	Incoming/outgoing calls, durations, and voicemail messages are recorded. Calls are not recorded. Telephones are tagged with room locations for emergency response (911) purposes.	Passive (Logs)

5.0 ROLES AND RESPONSIBILITIES

5.1 The employer must provide a copy of the Electronic Monitoring Policy to all existing employees within 30 calendar days of:

5.1.1 The day the employer must have the policy in place, or

5.1.2 An existing policy being changed.

5.2 The employer must provide a copy of the Electronic Monitoring Policy within 30 days of the later of either:
  5.2.1 The day the employer must have the policy in place, or
  5.2.2 The day the individual becomes an employee of the employer.
5.3 A printed or electronic copy of the policy may be provided to employees. If providing an electronic copy such as an e-mail attachment or an online link, the employer will ensure that the employee has access to a printer.

6.0 INTERPRETATION

Questions of interpretation or application of this policy or its procedures will be referred to:

Director of Information Technology
935 Ramsey Lake Rd.
Sudbury ON
P3E 2C6
705-662-7130
it.director@nosm.ca

7.0 RELATED DOCUMENTS

University Documents and Information

- Acceptable Use of Information Technology Policy
- Handling Sensitive Electronic Information Policy

Legislation and Information

- Employment Standards Act, 2000, S.O. 2000
- Bill 88, Working for Workers Act, 2022

AUTHORITIES AND OFFICERS

The following is a list of authorities and officers for this policy:
a. Approving Authority: Executive Group
b. Responsible Officer: VP Administration and COO
c. Procedural Authority: Director, Information Technology
d. Procedural Officer: Director Information Technology

Review and Revision History

Review Period: 3 years or as required

Date for Next Review: 2025