Brock University

ELECTRONIC MONITORING POLICY

PURPOSE

The purpose of this Policy is to outline Brock University's use of electronic monitoring tools for employee activity and reflects the University's commitment to transparency regarding electronic monitoring and compliance with the *Employment Standards Act, 2000*.

This Policy is intended to outline the University's Electronic Monitoring practices and should be read in conjunction with other applicable University policies, guidelines or standards.

SCOPE

This Policy applies to all Employees of Brock University.

If any provision of this Policy is inconsistent with the provisions of a collective agreement, the collective agreement will prevail, unless the Policy provision is required by law, in which case the Policy provision will prevail.

POLICY STATEMENT

1- Brock University uses various Electronic Monitoring tools in different circumstances and for different purposes. However, the University does not actively monitor Employees using electronic means for the purpose of Employee performance management as an ordinary course of business.

2- This Policy does not provide Employees with any new privacy rights or a right to not be electronically monitored. Nothing in this Policy affects or limits the University's ability to conduct, or use information obtained through, Electronic Monitoring.

3- The University categorizes its Electronic Monitoring practices into two groups:

- Active Electronic Monitoring
- Passive Electronic Monitoring

4- The University may use data collected from Electronic Monitoring for employment-related purposes and reserves any and all rights to do so.

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

6- In the event, 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 applicable legislation, including, but not limited to, FIPPA.

7- Appendix (A) outlines how and in what circumstances the University uses Electronic Monitoring tools and the purposes for which information obtained through Electronic Monitoring tools may be used by the University. Appendix (A) may be updated from time to time. Notice will be provided to University employees within 30 days of such updates being made.

DEFINITIONS

Active Electronic Monitoring is the use of Electronic Monitoring tools that are intended to intentionally track Employee activity or location and is monitored in real-time or in close proximity to the time of collection. For example, please see Appendix (A). Active Electronic Monitoring may involve human intervention and is executed to investigate alerts or incidents.

CSIRT: Computer Security Incident Response Team.

Electronic Monitoring Electronic Monitoring includes "all forms of Employee monitoring that is done electronically." Electronic Monitoring is not limited to the devices or monitoring equipment issued by the University or Electronic Monitoring that happens while Employees are on-site at a workplace.

Employee under this Policy means only those Employees of the University who are considered Employees under the *Employment Standards Act, 2000*.

Metadata: Data that provides information about other data.

Passive Electronic Monitoring is the collection, analysis and/or retention of data that may include, without limitation, data about Employee activity or location either in physical spaces or on the University's network that is not actively monitored. For examples, please see Appendix (A). The University conducts passive Electronic Monitoring of physical spaces and digital identities, assets, and resources. Passive Electronic Monitoring usually does not involve humans and is typically engaged by software, devices or cloud services to hunt for anomalous, risky or suspicious behaviour to alert administrators.

COMPLIANCE AND REPORTING

(a) The University shall provide a copy of this Policy to each Employee, regardless of their position, within 30 calendar days of implementation. Should any changes be made to the Policy after its implementation, the University shall provide each Employee of the University a copy of the revised Policy within 30 days of the changes being made.

(b) The University shall provide a copy of this Policy to all new Employees within 30 calendar days of the Employee commencing employment with the University.

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

This Policy is under the jurisdiction of Vice-President, Administration. The interpretation and application of this Policy is the responsibility of Human Resources.

Information Table format (see example below):

Policy Owner:	Vice-President, Administration
Policy Lead:	Associate Vice-President, Human Resources
Policy Classification:	Operational
Approval:	Approved by the Executive Team
Effective date:	October 11, 2022
Next review:	October 2025
Revision history:	Adopted October 2022
Related documents:	Employment Standards Act, 2000 Access to Information and Protection of Privacy Policy

Appendix (A) Electronic Monitoring tools and the purposes

Tool	Type	When	Who processes	How	What	Purpose
Attendance Management	Active	Daily	ITS	Software	Recording attendance	Track Employee work hours and attendance
Facility Management System	Active	Daily	Facilities	Software	Workplace management system	Track assigned maintenance work orders and completion rate / Employee in addition to space planning
Security Information and Event Management (SIEM)	Active	During investigations for alerts regarding suspicious or risky activities	ITS CSIRT, ITS Infrastructure	Software tracks events generated by devices or software	Metadata of device network traffic, logs of devices, software or services	Information Security, Incident Response
Security Information and Event Management (SIEM)	Continuous, Passive	Day to day operations	ITS CSIRT, ITS Infrastructure	Software tracks and generates alerts for suspicious or risky events	Metadata of device network traffic, logs of devices, software or services	Information Security, Incident Response
Email Monitoring	Continuous, Passive	Day to day operations	ITS CSIRT	Software tracks and generates alerts for suspicious or risky events	Metadata of emails including originating sender IP, sender address, receiver address, subjects, URLs and attachment file names	Information Security, Incident Response

Email Monitoring	Active	When investigating alerts regarding suspicious or risky activities	ITS CSIRT	Software tracks and generates alerts for suspicious or risky events	Metadata of emails including originating sender IP, sender address, receiver address, subjects, URLs and attachment file names	Information Security, Incident Response
Endpoint Detection and Response	Continuous, Passive	Day to day operations	ITS CSIRT	Software tracks and generates alerts for events regarding the usage of endpoints	Metadata of system execution	Information Security, Incident Response
CCTV/Video Camera Systems	Continuous, Active	Day to day operations	Campus Security	Cameras record video footage of specific areas within the University's facility	Video footage	Facility Security
VPN	Continuous, Passive	Day to day operations	ITS CSIRT, ITS Infrastructure	Software records device connectivity	Metadata of device connectivity including source IP, destination IP, source port, destination port	Network Security
Anti-virus software	Continuous, Passive	Day to day operations	ITS CSIRT, ITS Desktop Services, ITS Infrastructure	Software monitors device activity and alerts on suspicious or risky behavior	Device activity pertaining to files on the system and resources accessed by the user	Endpoint Security
Wired connectivity	Continuous, Passive	Day to day operations	ITS Infrastructure , ITS CSIRT	Devices monitor device connectivity activity	Device mac address, device IP address, user associated with device, infrastructur	Network Security, Service Assurance

					e asset user is connecting to	
Wireless connectivity	Continuous, Passive	Day to day operations	ITS Infrastructure, ITS CSIRT	Devices monitor device wireless connectivity activity	Device mac address, device IP address, user associated with device, infrastructure asset user is connecting to	Network Security, Service Assurance
Web applications	Continuous, Passive	Day to day operations	ITS Infrastructure, ITS CSIRT, ITS Enterprise Services	Software monitors device connectivity activity, Software uses a unique number to identify a user	Source IP, URL accessed, Destination site, Cookie. User activities	Information Security, Web Session Tracking.
Authentication Systems	Continuous, Passive	Day to day operations	ITS CSIRT	Software records authentication metadata of identity and access management events	Authentication event metadata	Information Security
File Servers	Continuous, Passive	Day to day operations	ITS CSIRT	Software monitors user access to files	File access events metadata	Information Security
Remote Access Tools (Bomgar)	Continuous, Passive	Day to day operations	ITS Infrastructure, ITS Desktop Services	Software monitors remote access activity to university assets	Remote access event metadata, session recordings	Information Security
Remote Access Tools (Bomgar)	Active	When investigating issues or actions associated to sessions recorded by Bomgar	ITS Infrastructure, ITS Help Desk	Software monitors remote access activity to university assets	Remote access event metadata, session recordings	Information Security, Service Provider Management
Print Servers	Continuous, Passive	Day to day operations	ITS Infrastructure, ITS Desktop Services	Software monitors print jobs sent by users to printers	Print job metadata	Audit Logs

Mail Campaign Tools	Continuous, Passive	Day to day operations	Marketing and Communications	Software monitors user interaction with email campaigns	User interaction metadata	ITS Identify clients interaction for marketing purposes
Telephone Systems	Continuous, Passive	Day to day operations	ITS infrastructure	Software records metadata of all calls sent or received. Some calls may be recorded or monitored.	Metadata of calls, Calls recorded	Billing, quality assurance
Closed Circuit Television	Active/Passive	24/7	CSS Dispatchers	Panasonic Recording Software	Video Footage -file type -live monitoring -no audio	-Safety and Security -emergencies -investigations
Blue Butler Recording software	Active/Passive	Incoming/outgoing calls, radio transmission	CSS Dispatchers	Recording software	Audio, phone #,date, time, duration of call	-Emergencies -investigations
Student Management Systems	Passive	Upon request/ investigation	Registrar Office	Software tracking changes, dates and times. Live chat platform. email	Tracking changes, who made the changes, type of changes, date and time	Track completion rate and individual completed the tasks, pending tasks
Learning Management System	Continuous, Passive	Day to day operations	ITS Infrastructure, ITS CSIRT, CPI	Software monitors device connectivity activity, Software uses a unique number to identify a user	Source IP, URL accessed, Destination site, Cookie. User activities	Information Security, Web Session Tracking. Performance measures