TORONTO POLICE SERVICES BOARD

ELECTRONIC MONITORING

APPROVED	09/13/2022	Minute No: P2022-0913-3.0.
REVIEWED (R) AND/OR AMENDED (A)		
REPORTING REQUIREMENT		
LEGISLATION	*Employment Standards Act, 2000*, S.O. 2000, c. 41, Part XI.1	

PURPOSE OF POLICY

The purpose of this Electronic Monitoring Policy (the "Policy") is to describe how and in what circumstances the Employer may electronically monitor Employees, and to outline the purposes for which information obtained through electronic monitoring may be used. "Electronic monitoring" refers to employee monitoring that is conducted electronically.

APPLICATION

This Policy applies to civilian Members of the Toronto Police Service (the "Service") and to Toronto Police Services Board Staff. For greater clarity, this Policy applies solely to all employees of the Toronto Police Services Board (the "Board"), as defined by the Ontario *Employment Standards Act, 2000* (collectively "Employees").

For the purposes of this Policy, the term "Employer" refers to the Board and/or Service, as applicable.

The Policy should be read in conjunction with other applicable Board Policies, Service Procedures, guidelines, and standards, including, but not limited to:

- Standards of Conduct
- Affirmation/Oath of Secrecy
- Information Security Policy
- Core Values
- Guidelines for Remote Work and Remote Work Member Agreement
- Conduct of Service Members
- Records Retention Schedule
- Closed Circuit Television (CCTV) Program
- Procedure 04-46 Closed Circuit Television (CCTV)
- Procedure 15-11 Use of Service Vehicles
- Procedure 15-17 In Car Camera System

- Procedure 15-18 Secure Laptop
- Procedure 15-20 Body-Worn Camera
- Procedure 17-02 Information Breaches
- Procedure 17-11 Toronto Police Service Intranet
- Procedure 17-12 Service Communication Systems

DEFINITIONS

For the purpose of this Policy, the following definitions apply:

Video/Audio Surveillance/Monitoring Equipment: Surveillance or otherwise monitoring by means of a camera or other recording device that monitors or records visual images and/or captures audio of activities recorded on Employer-owned electronic devices. This includes, but is not limited to, on-site surveillance cameras, in-car camera systems, and body-worn cameras.

Computer Monitoring: The practice of collecting user activity data on Employer-owned computers, tablets, Connected Officer devices, networks, and other IT infrastructure. This data includes, but is not limited to, web browsing history, files downloaded, data input, network traffic, logons to corporate systems, interactions with data, peripheral device usage (mouse, keyboard, monitor, etc.), and information about the Employee's computer.

Electronic Access Controls (EACs): The technology used to provide and deny physical or virtual access to a physical or virtual space. This includes, but is not limited to, the magnetic stripe included within proximity/ID access cards, which also keeps records of access times and locations.

Global Positioning System (GPS): A network of satellites and receiving devices used to determine the location of something on Earth. This technology can be enabled within equipment such as vehicles [Automated Vehicle Location System (AVLS)], Connected Officer devices, and portable radios, in order to determine the location of the equipment, both at present, and historically. AVLS also documents current and historical speed of vehicles in which it is enabled.

GUIDING PRINCIPLES

Expectation of Privacy in the Workplace

Monitoring Employee usage of Employer-owned workplace technology devices is an essential component of enforcing Procedures, maintaining a respectful work environment, and ensuring that Information Technology (I.T.) assets that are owned and managed by the Employer are used safely and appropriately. This includes an Employee's personal device when operated on the Remote Desktop Connection desktop-as-a-service platform. The Employer monitors workplace technology devices to ensure I.T. resources are used in accordance with the *Information Security Policy, Information Security Guidelines,* and other relevant Board Policies, guidelines and Service Procedures.

For that reason, **Employees must not expect privacy when using Employer systems.** While all personal information collected by the Employer will be used fairly and appropriately as per this Policy, all activities that take place via Employer-owned electronic assets should be considered monitored.

Types of Employee Monitoring Conducted and Their Purpose

The Employer uses various electronic tools to monitor Employees for different purposes.

a) Video/Audio Surveillance/Monitoring

Video/audio surveillance/monitoring equipment is used on a continuous basis on Employer premises to ensure that Employees and visitors are provided with a safe and secure environment, as well as to ensure that Employer-owned assets are kept secure from theft, vandalism, and other forms of misconduct.

Video/audio surveillance/monitoring equipment will not be used in areas where Employees have a reasonable expectation of privacy, such as bathrooms, changing rooms, and other private areas. Where video/audio surveillance equipment is used, the equipment will be made clearly visible and there will be notices indicating the presence of the equipment.

Employees may also be subject to video/audio surveillance/monitoring on and off Employer facilities at any time during the course of performing their regular job duties. This includes Closed Circuit Television (CCTV), in-car camera systems (ICCS), body-worn cameras (BWC), Connected Officer devices, and Service communications systems. Use of this equipment is monitored to ensure resources are used in accordance with relevant Employer Procedures.

b) Computer Monitoring

The Employer monitors the network and computer activity of Employees to ensure that Employer-owned I.T. resources (including email communications, instant messages and facsimiles) are used in accordance with the *Information Security Policy, Information Security Guidelines* and other Board Policies, guidelines and Service Procedures where relevant. I.T. systems continually log activities while devices are on and connected to the Internet. All logs are stored in the Employer's centralized audit log repository. Employees who are utilizing the Remote Desktop Connection desktop-as-a-service platform are subject to the same monitoring while accessing the Employer's virtual desktop.

I.T. systems are capable of accessing system information, as well as all information and data stored and communicated through I.T. resources. For example, all email communications, instant messages and facsimiles that are sent through Employer-owned networks, equipment, or user accounts are automatically logged, and at any time, are subject to monitoring and audit to ensure appropriate usage. This may include personal email accounts when those accounts are accessed through Employer-owned I.T. assets.

Computer activity data collected through electronic monitoring may be used to facilitate work in an Employee's absence, to evaluate an Employee's performance, to detect malicious or high-risk activities, to monitor network performance and to prevent security incidents from occurring. Data collected may also be subject to evidence in a workplace investigation or Freedom of Information request.

The Employee monitoring measures put in place capture the following data:

- Timestamps of computer power states: startup, shutdown, and sleep events
- Logons on Employer computers, virtual machines, and other desktops
- Logs of peripheral devices used on a given endpoint, such as storage devices (USB, DVD/CD, Tape, SD Card, etc.), wireless devices, communication ports, imaging devices, and mobile phones
- Documents sent to a printer and copies of documents made and sent
- File operations to portable storage devices (files copied, created, renamed, and/or deleted to/from these devices)
- Internet usage data, including URLs/domains, pre-defined website content category, web page headers, search engine queries, timestamps, bandwidth consumption, and browsing time
- Application usage, including software downloads, and time spent using each software
- Screenshots of activities performed on Employer-owned workstations through the Employer centralized audit log repository
- IP addresses and system information of client computers

c) Telephone Monitoring

All Employer-owned mobile and landline phones may be monitored to ensure appropriate usage and compliance with the Board's Policy and Service Procedures regarding the use of telephones in the workplace.

All calls made from Employer landlines are automatically logged and information regarding the caller/recipient, location of phone, and duration are recorded onto telephone provider hardware. Telephone conversations may be recorded.

When an Employee accesses any Employer software through their Employer-owned mobile phones, information is automatically catalogued, by means of Employer auditing systems, with respect to what information is accessed and communicated through I.T. resources.

All Employer-owned mobile devices are equipped with Global Positioning System (GPS) that are able to access the device's location, which may assist the Employer in locating a lost or stolen device.

If a personal mobile device is used for work purposes, phone calls will not be monitored unless they are made through Employer-provided mobile applications that are provided for the purpose of making work-related calls.

Telephone data and information from a cell phone's forensic extraction may be used to locate a missing or stolen device, detect malicious or high-risk activities, and to prevent security incidents from occurring.

d) *Electronic Access Controls (EACs)*

Information obtained from the use of EACs (such as proximity/ID access cards) is automatically recorded upon an Employee scanning or tapping their ID access card. This information may be used to ensure compliance, and to assist in the investigation of theft, accident, or other incidents.

e) Global Positioning System (GPS)

GPS data is automatically collected when Employer devices, such as smartphones and Employer vehicles, are turned on and connected to the internet or a mobile network. Data acquired through the use of GPS in Employer-issued equipment is recorded and monitored for purposes related to the location of Employer-owned assets, such as mobile devices and vehicles, for the retrieval of lost or stolen property, driver safety, vehicle maintenance, driver behaviour, and patrol coverage.

Data Retention

To ensure that all personal information is only kept for as long as it is necessary to do so, all data that is captured as a result of workplace monitoring will be stored digitally on Employer-owned servers, as well as Cloud servers, in accordance with the Records Retention Schedule. Personal information will only be stored for a greater period of time under exceptional circumstances, or as required by law, including (but not limited to) retention of data related to criminal conduct, internal investigations, civil litigation, Special Investigations Unit requests, and Freedom of Information requests.

Unlawful Activity, Discipline, and/or Termination of Employment

In addition to the purposes listed above, the Employer may rely on information collected through electronic monitoring to discipline or terminate the employment of an Employee.

Information collected by electronic monitoring tools may be used for the purposes of monitoring, evaluating or investigating Employee performance, behaviour or conduct.

Nothing in this Policy affects or limits the Employer's ability to use or disclose information obtained through electronic monitoring in accordance with any applicable laws, regulations, collective agreements, or contracts.

POLICY OF THE BOARD

It is the policy of the Board that:

1. All Employees acknowledge that there is no expectation of privacy when using Employer systems, including Employer-owned computers, tablets, Connected Officer devices, networks, and other I.T. infrastructure;

2. The Employer is authorized to electronically monitor Employees through the use of video/audio surveillance/monitoring equipment, computer monitoring, telephone monitoring, Electronic Access Controls and Global Positioning Systems, as outlined in this Policy, and for the purposes detailed in this Policy;

3. The Chief of Police will ensure that all data that is captured as a result of workplace monitoring will be stored digitally on Employer-owned servers, as well as Cloud servers, in accordance with the Employer's Records Retention Schedule;

4. The Chief of Police may rely on information collected through electronic monitoring to discipline or terminate the employment of an Employee;

5. The Chief of Police, in regards to civilian Members of the Toronto Police Service, and the Executive Director, in regards to employees of the Toronto Police Services Board, will ensure that Unit Commanders take all reasonable steps to ensure Employees under their management are aware of the information included within this Policy;

6. The Chief of Police, in regards to civilian Members of the Toronto Police Service , and the Executive Director, in regards to employees of the Toronto Police Services Board, will ensure that:

    a. All new Employees are provided with a copy of this Policy within 30 days of their hire date; and

    b. All existing Employees are provided with a copy of this Policy, and any amended versions of this Policy, within 30 days of approval or amendment; and

7. The Employer will retain a copy of this Policy for three (3) years after the Policy ceases to be in effect.