	ELECTRONIC MONITORING POLICY #11.3
CATEGORY: IT Services	**APPROVAL DATE:**
EFFECTIVE DATE: October 11, 2022	**REVIEW DATE:** three (3) years from approval date
APPROVAL: OCAD U Executive Team	
OFFICE OF ACCOUNTABILITY: IT Services	
ADMINISTRATIVE RESPONSIBILITY: Chief Information Officer	
PREVIOUS VERSIONS: None	

OCAD University is committed to transparency with regard to electronic monitoring. The purpose of this policy is to clearly communicate the University's use of electronic monitoring tools and meet the updated requirements under the *Employment Standards Act, 2000*.

The University does not proactively monitor employees for the purpose of tracking individual movement or as a normal course of evaluating performance. Active and passive electronic monitoring does take place in order support the safety of people and assets on campus.

In unique circumstances, existing electronic monitoring tools could be used to conduct investigations as a result of allegations made or other legal requirements. The University may use data collected from active or passive electronic monitoring tools for employment-related purposes and reserves the right to do so.

Application

This policy applies to all employees, including both academic and administrative staff and management, and should be read in concert with other administrative policies, including the IT Acceptable Use Policy, Email Policy, and the Information & Data Classification Policy, as well as applicable collective agreements and laws.

Electronic Monitoring Practices

The University categorizes its electronic monitoring practices into two groups:

Active Electronic Monitoring

Active monitoring refers to the use of electronic tools that are intended to track employee activity or location and is monitored in real-time or close proximity to the time of collection. For example, active electronic monitoring tools include security cameras, card readers for access to physical locations and end point protection to address cyber security risks.

Passive Electronic Monitoring

Passive monitoring refers to 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. Examples of passive electronic monitoring tools include email and network security logs.

The following table outlines how and in what circumstances the University uses electronic monitoring tools, and the primary purposes for which the information may be used:

Electronic Monitoring Tool	**Circumstances in Which Electronic Monitoring May Occur**	**How Electronic Monitoring Occurs**	**Primary Purpose For Which the Collected Information May Be Used**
IT security software	Continuous	Software tracks and triggers events for suspicious or risky user activity.	Network security
Electronic communications	Continuous	Software records copies of all messages sent or received by addresses within the University's domain.	Network security
Electronic key fob/access badge systems	Each scan	An electronic sensor creates a record each time an authorized user scans their key fob and enters the University's premises or specific facilities.	Facility security
Firewalls/VPN/Web Gateways	Continuous	Network security programs and tools to monitor use and access of University systems and networks.	Network security
Endpoint threat detection and response tools	Continuous	"ETDR" monitors the use of workstations (programs run, files read and written, etc.) and	Network security

Electronic Monitoring Tool	**Circumstances in Which Electronic Monitoring May Occur**	**How Electronic Monitoring Occurs**	**Primary Purpose For Which the Collected Information May Be Used**
		compares it against a baseline to detect abnormalities and potential unauthorized use.	
CCTV/Video Camera Systems (facilities)	Continuous	Cameras record video footage of specific areas within the University's facility.	Facility security, employee and asset protection

Note: The University is subject to the requirements of the *Freedom of Information and Protection of Privacy Act* (FIPPA). and must collect, use and disclose personal information in accordance with applicable legislation, including, but not limited to, FIPPA.