

ADM 111

POLITIQUE EN MATIÈRE DE SURVEILLANCE ÉLECTRONIQUE

CONSEIL D'ADMINISTRATION DE L'UNIVERSITÉ DE HEARST

**DATE D'ENTRÉE EN
VIGUEUR** octobre 2026

**DERNIÈRE DATE DE
RÉVISION** 14 octobre 2026

**DERNIÈRE DATE
D'ADOPTION** 26 octobre 2026

**PROCHAINE DATE DE
RÉVISION** janvier 2029

*Cette politique relève, sous recommandation du comité
de gouvernance et d'éthique, du conseil d'administration
de l'Université de Hearst.*

*Pour obtenir ce document sous un autre format accessible,
veuillez communiquer avec le vice-rectorat à l'administration.*

**Campus
de Hearst**

60, 9^e Rue
Hearst (Ontario) P0L 1N0

**Campus
de Kapuskasing**

7, rue Aurora
Kapuskasing (Ontario) P5N 1J6

**Campus
de Timmins**

395, boulevard Thériault
Timmins (Ontario) P4N 0A8

uhearst.ca
1 800 887-1781

Table des matières

1. Préambule	3
2. Champ d'application	3
3. Définitions	3
4. Pratiques de surveillance électronique	4
4.1. Systèmes informatiques	5
4.2. Système de vidéosurveillance	5
4.3. Tableau des pratiques	5
5. Lois, politiques, règlements et autres documents connexes	6
6. Révision de la politique	6

1. Préambule

Conformément aux exigences de la **Loi de 2000 sur les normes d'emploi (Ontario)**, l'Université de Hearst adopte la présente politique afin d'informer les membres du personnel des pratiques de surveillance électronique pouvant être exercées dans le cadre de ses activités.

La présente politique vise notamment à :

- satisfaire aux exigences prévues par la Loi de 2000 sur les normes d'emploi concernant les politiques de surveillance électronique;
- informer les membres du personnel des formes de surveillance électronique pouvant être exercées par l'Université;
- préciser les circonstances dans lesquelles une surveillance électronique peut être effectuée;
- décrire les outils de surveillance électronique utilisés;
- expliquer les fins auxquelles les renseignements recueillis peuvent être utilisés;
- favoriser une utilisation responsable, transparente et proportionnée des technologies de surveillance;
- protéger les personnes, les renseignements, les systèmes d'information et les biens de l'Université.

La présente politique constitue une mesure d'information destinée aux membres du personnel. Elle ne modifie ni ne limite les droits et obligations de l'Université ou des membres du personnel prévus par la loi, les conventions collectives, les contrats de travail ou les politiques institutionnelles applicables.

La présente politique est adoptée conformément à la Loi de 2000 sur les normes d'emploi (Ontario). Elle est fournie à titre informatif et ne crée aucun droit supplémentaire à l'égard de la vie privée ni aucune restriction aux droits de gestion de l'Université, sous réserve des lois applicables.

2. Champ d'application

La présente politique s'applique à l'ensemble des membres du personnel de l'Université de Hearst, qu'ils occupent un emploi permanent, temporaire, contractuel, à temps plein ou à temps partiel, ainsi qu'aux personnes utilisant les systèmes, équipements ou infrastructures technologiques de l'Université dans le cadre de leurs fonctions.

3. Définitions

Surveillance électronique : Toute forme de surveillance d'un membre du personnel effectuée au moyen d'un dispositif, d'un système ou d'une technologie électronique.

Outils de surveillance électronique : Les systèmes, équipements, applications, réseaux, appareils ou autres ressources technologiques de l'Université pouvant permettre la collecte,

l'enregistrement, la conservation ou l'analyse de renseignements relatifs aux activités d'un membre du personnel.

Surveillance active : S'entend du suivi d'activités et d'événements, habituellement en temps réel, y compris, entre autres, les journaux d'audit, les fichiers audio et vidéo, les séquences filmées, les journaux d'entrée physique et les renseignements sur la localisation qui sont activement examinés régulièrement.

Surveillance passive : S'entend de la collecte de données, d'activités et d'événements par des systèmes automatisés visant à maintenir les opérations. Les données recueillies servent à détecter et régler un problème technique ou à fournir une analyse rétrospective. La surveillance passive peut aussi inclure la « présence » identifiable ou la disponibilité de renseignements qui peuvent avoir le statut « libre ou occupé » dans les calendriers en ligne, les suites de clavardage ou de collaboration.

4. Pratiques de surveillance électronique

L'Université peut effectuer certaines formes de surveillance électronique dans le cadre normal de ses activités afin :

- d'assurer la sécurité des personnes et des biens;
- de protéger les infrastructures technologiques;
- de prévenir, détecter ou enquêter sur des incidents de sécurité;
- de maintenir l'intégrité et le bon fonctionnement de ses systèmes;
- de satisfaire à ses obligations légales ou réglementaires.

Les renseignements recueillis peuvent être utilisés notamment :

- pour assurer la cybersécurité;
- pour enquêter sur un incident de sécurité, un accès non autorisé ou une activité frauduleuse;
- pour protéger les biens et les renseignements de l'Université;
- pour répondre à une demande des autorités compétentes lorsque la loi l'exige;
- pour soutenir une enquête administrative ou disciplinaire lorsqu'il existe des motifs raisonnables de croire qu'une politique, une procédure, une convention collective ou une obligation légale n'a pas été respectée.

L'Université n'effectue pas de surveillance électronique continue des membres du personnel dans le but d'évaluer leur rendement ou leur productivité. Toutefois, les renseignements recueillis dans le cadre normal de l'exploitation des systèmes peuvent être utilisés lorsqu'ils sont pertinents à une enquête, à une procédure disciplinaire ou à toute autre fin institutionnelle directement liée à la raison pour laquelle les renseignements ont été recueillis, conformément aux lois et politiques applicables.

4.1. Systèmes informatiques

Les systèmes informatiques de l'Université font l'objet d'une surveillance visant à assurer leur sécurité, leur disponibilité et leur bon fonctionnement. Cette surveillance comprend notamment la collecte automatisée de journaux d'activité, de données techniques et d'événements de sécurité permettant notamment de détecter les logiciels malveillants, les tentatives d'hameçonnage, les accès non autorisés ou d'autres menaces à la sécurité informatique.

Les renseignements ainsi recueillis sont généralement consultés uniquement lorsque cela est nécessaire afin d'assurer la sécurité des systèmes, d'effectuer un diagnostic technique ou d'enquêter sur un incident.

La surveillance électronique doit être conçue et utilisée de manière à respecter la liberté académique, l'autonomie professionnelle, la confidentialité des activités de recherche et les droits de propriété intellectuelle. Elle ne doit pas être utilisée à des fins de surveillance générale, d'évaluation ou de contrôle des activités académiques, professionnelles ou de recherche. Toute surveillance susceptible de concerner ces activités doit être nécessaire, proportionnée, limitée à une finalité déterminée et effectuée conformément aux lois applicables, aux conventions collectives, aux contrats d'emploi et aux politiques institutionnelles pertinentes. Elle ne peut être autorisée que pour répondre à une obligation légale, à un risque sérieux pour la sécurité ou l'intégrité des personnes, des systèmes ou des renseignements, ou à une enquête dûment justifiée, et l'accès doit être limité aux renseignements strictement nécessaires.

4.2. Système de vidéosurveillance

L'Université se sert d'un système de vidéosurveillance en circuit fermé pour assurer la sécurité de ses locaux et prévenir les délits (y compris les vols et le vandalisme ou autres dommages criminels). Des caméras sont installées dans ses locaux ainsi qu'à l'extérieur, près de l'entrée permettant d'accéder à ses locaux et à son immeuble. L'Université n'effectue pas de vidéosurveillance dans des espaces privés comme les toilettes.

Les enregistrements vidéo sont consultés uniquement lorsque cela est raisonnablement nécessaire pour les fins décrites dans la présente politique ou lorsque la loi l'exige.

4.3. Tableau des pratiques

L'Université ne surveille pas activement les membres du personnel par voie électronique aux fins de la gestion de rendement.

Catégorie	Type de surveillance	Type d'enregistrement	Utilisation des renseignements
Caméras de sécurité	Passive	Vidéo	Sécurité des personnes et des biens, enquête sur incident

Badges d'accès	Passive	Journal électronique	Contrôle des accès, sécurité des immeubles, enquête sur incident
Journaux réseau	Passive	Journaux système	Cybersécurité, diagnostic, conformité
Système de téléphonie	Passive	Journaux système	Sécurité, diagnostics
Système d'impression	Passive	Journaux système	Diagnostics, conformité
Comptes et courriels institutionnels	Passive	Journaux techniques	Sécurité, prévention des cyberattaques, diagnostics

5. Lois, politiques, règlements et autres documents connexes

- [*Loi de 2000 sur les normes d'emploi en Ontario*](#)
- [*Loi de 2022 visant à œuvrer pour les travailleurs*](#)
- [*Article 41.1.1 - Politique écrite sur la surveillance électronique*](#)
- ADM 102 - Politique sur l'accès à l'information et la protection de la vie privée - LAIPVP
- ADM 102a - Avis de collecte de renseignements à l'intention des étudiantes, des étudiants et du personnel de l'Université de Hearst
- ADM 106 - Politique sur la gestion des comptes de messagerie et des plateformes numériques
- ADM 109 - Politique sur la cybersécurité et la sécurité de l'information numérique (y compris les procédures liées à ladite politique)
- La déclaration des droits et des responsabilités du corps étudiant de l'Université de Hearst

6. Révision de la politique

La présente politique doit faire l'objet d'une révision à tous les trois (3) ans. Toute modification à la présente politique est recommandée au comité permanent de gouvernance et d'éthique, puis présentée au conseil d'administration de l'Université de Hearst pour son adoption.