Université de Sherbrooke

Centre de formation en technologie de l'information

INF 807 – Criminalistique en sécurité des TI

Plan d'activité pédagogique

Hiver 2026

Enseignants	Michel Céré	Marie-Eve Girard
Courriel :	michel.cere@usherbrooke.ca	marie-eve.girard9@usherbrooke.ca
Local :	Longueuil : L1-15741, Sherbrooke : D4-1010-15	
Téléphone :		
Disponibilités :	Sur rendez-vous, les personnes enseignantes pourront être disponibles en personne avant et après les séances ou par vidéoconférence Teams. Lors de ces rencontres, la caméra vidéo ainsi que le son audio seront obligatoires.	

Site web du cours : https ://moodle.usherbrooke.ca

Horaire Exposé magistral : Jeudi 18 h 30 à 21 h 50 salle Réunion Microsoft Teams

Description officielle de l'activité pédagogique[1]

Cibles de formation :	Comprendre les différentes étapes d'une enquête de piratage. Faire l'analyse de mémoire vive. Utiliser des outils de diagnostic pour repérer du code malveillant.
Contenu :	Principes de base de la criminalistique. Introduction aux outils de criminalistique en cours d'opération (forensic live), mémoire et statique des disques durs. Ingénierie inverse.
Crédits	3
Organisation	3 heures d'exposé magistral par semaine 6 heures de travail personnel par semaine
Particularités	Aucune

[1] https ://www.usherbrooke.ca/admission/fiches-cours/inf807

1 Présentation

Cette section présente les cibles de formation spécifiques et le contenu détaillé de l'activité pédagogique. Cette section, non modifiable sans l'approbation du comité de programme du Centre de formation en technologie de l'information, constitue la version officielle.

1.1 Mise en contexte

À la fin de cette activité pédagogique, l'étudiante ou l'étudiant sera capable :

1. Comprendre la criminalistique, son importance dans les organisations ainsi que la gouvernance et les bonnes pratiques auxquelles elle peut recourir.
2. Connaître les principes de base du droit criminel canadien et les crimes liés aux technologies.
3. Évaluer si les règles de sécurité minimale en matière de criminalistique sont présentes et suffisantes.
4. Comprendre les différentes étapes d'une enquête lors d'un incident de sécurité.
5. Connaître les règles et mécanismes de conservation de la preuve numérique en droit criminel canadien.
6. Connaître les mécanismes d'utilisation de la preuve numérique et du témoignage d'un expert dans le cadre d'un procès criminel.
7. Connaître différents enjeux liés à la capture et la conservation de la preuve en TI

1.2 Cibles de formation spécifiques

Le Microprogramme en sécurité informatique - volet réaction permet à l'étudiante ou à l'étudiant de :

- maîtriser la nature, le rythme et les outils des cyberattaques contre divers types d'infrastructure ;
- savoir détecter les signes et artefacts d'une intrusion, pouvoir mesurer son ampleur et pouvoir en déterminer la chaîne causale ;
- savoir dresser et exécuter un plan d'intervention en cas d'incident et de brèche de données, de manière à trouver le meilleur compromis entre la minimisation des dommages et l'interruption des activités de l'organisation.

1.3 Contenu détaillé

Thème	Contenu	Nbr. d'heures	Objectifs
1	Introduction et présentation du plan de cours	1	
2	Introduction aux concepts de droit pénal et criminel*	1	
3	Sources des besoins liés à la criminalistique*	1	
4	L'événement – Atelier*	1	
5	Les préalables à la criminalistique*	1	
6	Le processus d'enquête en criminalistique : L'identification*	1	
7	Le processus d'enquête en criminalistique : La cueillette*	1	
8	Conférence*	1	
9	Le processus d'enquête en criminalistique : L'examen*	1	
10	Le processus d'enquête en criminalistique : L'analyse*	1	
11	Le processus d'enquête en criminalistique : La présentation*	1	
12	La preuve numérique en matière criminelle et pénale*	1	
13	Enjeux liés à la capture de la preuve et sa conservation en TI*	1	
14	Révision de la matière - Conférence*	1	

2 Organisation

Cette section propre à l'approche pédagogique de chaque enseignante ou enseignant présente la méthode pédagogique, le calendrier, le barème et la procédure d'évaluation ainsi que l'échéancier des travaux. Cette section doit être cohérente avec le contenu de la section précédente.

2.1 Méthode pédagogique

Plusieurs méthodes pédagogiques seront utilisées pendant le cours, notamment celles qui sont décrites ci-dessous.

Dans un premier temps, il est fortement recommandé d'être présent en classe lors du cours, au risque de ne pas être en mesure de capter les subtilités de certains concepts et ne pas bénéficier des exemples, discussions, modèles et schémas qui seront présentés par la personne enseignante.

Principalement, la méthode traditionnelle (magistrale) sera utilisée pour l'enseignement des concepts clés pendant le cours. Sur Moodle, les personnes étudiantes retrouveront les références au matériel complémentaire ou la source du matériel présenté en classe. Des documents pourraient également être disponibles sur Moodle ou sur Teams dans la section « Fichier » du canal pour le cours.

La méthode démonstrative ainsi que la méthode interrogative seront utilisées par le biais d'échanges, de discussions ou de débats qui auront lieu en classe. La participation et les échanges sont essentiels à l'apprentissage et encouragés. Le matériel supplémentaire, qu'il soit sur Moodle ou ailleurs, servira à approfondir ou à explorer davantage les concepts abordés en classe, mais ne les remplacera pas.

La méthode découverte sera principalement utilisée lors des travaux. Les personnes étudiantes se verront présenter les notions essentielles en classe ou à l'aide de lectures dont les références seront disponibles sur Moodle et ils devront ensuite cheminer dans la réalisation du travail.

2.2 Calendrier

Semaine	Commençant le	Thème	Activités
1	2026-01-05	1	Mini-test 1
2	2026-01-12		Mini-test 2
3	2026-01-19		Mini-test 3
4	2026-01-26		mini-test de conférence 1
5	2026-02-02		Mini-test 4
6	2026-02-09		Mini-test 5
7	2026-02-16		Mini-test 6
8	2026-02-23		mini-test de conférence 2
9	2026-03-02	Relâche	
10	2026-03-09	Projet	Atelier de révision pour les présentations
11	2026-03-16	Projet	Présentations d'équipe (thème 1)
12	2026-03-23	Projet	Présentations d'équipe (thème 2)
13	2026-03-30	Projet	Présentations d'équipe (thème 3)
14	2026-04-06		mini-test de conférence 3
15	2026-04-13	Révision	Examen à réaliser à la maison.
16	2026-04-20	Semaine des examens finals	
17	2026-04-27	Semaine des examens finals	

Les lectures sont disponibles sur le site Moodle du cours INF807. Elles peuvent être sous format PDF ou un format spécifique à Moodle (le format livre Moodle, page web, glossaire, wiki ou autre.). Afin de rendre le contenu plus accessible, certains documents

seront disponibles dans la section "Fichier" sur le canal Teams du cours.

Le contenu des séances peut varier en fonction de la disponibilité de certains conférenciers. Veuillez vous fier au calendrier des événements qui sera disponible sur Moodle pour le contenu détaillé des séances, les lectures, les notes de cours et les dates de remises pour les travaux, des mini-tests et des présentations.

2.3 Évaluation

Type de l'évaluation	Pondération	Utilisation des IAG[1]
Présentation individuelle ou d'équipe	25 %	Interdite
Mini-tests d'évaluation des séances de cours (6)	30 %	Interdite
Mini-test d'évaluation des conférences (3)	15 %	Interdite
Examen final	30 %	Interdite

[1] Référez-vous à la page "Balises d'utilisation des outils d'intelligence artificielle générative" à la fin du document.

DIRECTIVE CONCERNANT LES MINI-TESTS

Les mini-tests se feront sur la plateforme Moodle et devront être complétés avant la prochaine séance (donc le mercredi 23h59 au plus tard).

Afin de pouvoir répondre adéquatement aux questions liées aux conférences, la présence en ligne sera obligatoire pendant toute la période prévue pour celle-ci. Les conférences ne seront pas enregistrées et aucune reprise ne sera possible.

Les personnes devront tenir compte des imprévues techniques, des mises à jour et des périodes de non-disponibilité de la plateforme lorsqu'elles devront compléter les mini-tests.

DIRECTIVE PARTICULIÈRE CONCERNANT LES PRÉSENTATIONS D'ÉQUIPE

Une évaluation de la contribution des membres de l'équipe sera effectuée après les présentations et pourra affecter jusqu'à 100% du résultat de chaque membre.

DIRECTIVE GÉNÉRALE CONCERNANT LA PRODUCTION ÉTUDIANTE (INDIVIDUELLE OU D'ÉQUIPE)

Toute utilisation d'une intelligence artificielle générative dans une production étudiante ou d'équipe devra être accompagnée d'une déclaration à cet effet.

Une personne ou une équipe qui ne remplit pas le « Formulaire de déclaration de l'utilisation de l'intelligence artificielle générative dans une production étudiante » ou ne respecte pas le niveau d'utilisation autorisé par la personne enseignante, pourrait voir sa production rejetée et recevoir la note de zéro (0). De plus, une note à cet effet pourra être inscrite au dossier de la personne ou des membres de l'équipe.

2.3.1 Qualité de la langue et de la présentation

Conformément à l'article 17 du Règlement facultaire d'évaluations des apprentissages[2] l'enseignante ou l'enseignant peut retourner à l'étudiante ou à l'étudiant tout travail non conforme aux exigences quant à la qualité de la langue et aux normes de présentation.

2.3.2 Plagiat

Le plagiat consiste à utiliser des résultats obtenus par d'autres personnes afin de les faire passer pour sien et dans le dessein de tromper l'enseignante ou l'enseignant. Vous trouverez en annexe un document d'information relatif à l'intégrité intellectuelle qui fait état de l'article 9.4.1 du Règlement des études[3]. Lors de la correction de tout travail individuel ou de groupe une attention spéciale sera portée au plagiat. Si une preuve de plagiat est attestée, elle sera traitée en conformité, entre autres, avec l'article 9.4.1 du Règlement des études de l'Université de Sherbrooke. L'étudiante ou l'étudiant peut s'exposer à de graves sanctions qui peuvent être soit l'attribution de la note E ou de la note zéro (0) pour un travail, un examen ou une activité évaluée, soit de reprendre un travail, un examen ou une activité pédagogique. Tout travail suspecté de plagiat sera transmis au Secrétaire de la Faculté des sciences. Ceci n'indique pas que vous n'ayez pas le droit de coopérer entre deux équipes, tant que la rédaction finale des documents et la création du programme restent le fait de votre équipe. En cas de doute de plagiat, l'enseignante ou l'enseignant peut demander à l'équipe d'expliquer les notions ou le fonctionnement du code qu'elle ou qu'il considère comme étant plagié. En cas d'incertitude, ne pas hésiter à demander conseil et assistance à l'enseignante ou l'enseignant afin d'éviter toute situation délicate par la suite.

2.4 Échéancier des travaux

Selon le nombre de participants au cours, les présentations seront individuelles ou en équipe. La présentation d'une durée de 20 minutes sera suivie d'une courte période d'échange. Le choix du thème et du sujet devra être identifié et confirmé auprès de la personne enseignante avant la 4e séance.

À titre indicatif, vous trouverez ci-dessous les thèmes des présentations avec un aperçu des différents sujets qu'il sera possible de présenter.

1. Thème : Les normes ou référentiels pertinents en criminalistique de la sécurité des TI
    - ISO 27037
    - ISO 27041
    - ISO 27042
    - ISO 27043
    - ISO 27050
    - NIST SP 800-86
    - Recommandations de l'IOCE
2. Thème : Outils de capture de la preuve technologique ou de gestion des dossiers d'enquête
    - Encase
    - Cellebrite
    - FTK
    - Autopsy
    - Magnet
    - SIFT Workstation
    - Wireshark
3. Thème : Utilisation de preuves numériques dans un procès criminel ou pénal - Exemples
    - R. c. Vu (2013)
    - R. c. Jones (2017)
    - R. c. Marakah
    - R. c. Cole (2012)
    - R. c. Morelli (2010)
    - R. c. Bykovets (2024)
    - R. c. Fearon (2014)

[2] https://www.usherbrooke.ca/sciences/fileadmin/sites/sciences/documents/Etudiants_actuels/Informations_academiques_et_reglements/2017-10-27_Reglement_facultaire_-_evaluation_des_apprentissages.pdf

[3] https://www.usherbrooke.ca/registraire/droits-et-responsabilites/reglement-des-etudes/

2.5 Utilisation d'appareils électroniques et du courriel

Selon le règlement complémentaire des études, section 4.2.3 [4], l'utilisation d'ordinateurs, de cellulaires ou de tablettes pendant une prestation est interdite à condition que leur usage soit explicitement permise dans le plan de cours.

Dans ce cours, l'usage de téléphones cellulaires, de tablettes ou d'ordinateurs est autorisé. Cette permission peut être retirée en tout temps si leur usage entraîne des abus.

Tel qu'indiqué dans le règlement universitaire des études, section 4.2.3[5], toute utilisation d'appareils de captation de la voix ou de l'image exige la permission de la personne enseignante.

Note : Je réponds aux questions posées par courriel à l'extérieur des périodes de cours.

Les communications officielles auront lieu principalement par courriel. Sinon, les communications usuelles, précisions ou questions relatives au cours ou aux travaux se feront sur Teams ou en personne lors des séances. La présence aux séances, bien que non obligatoire, est très fortement suggérée, car l'information qui pourra y être transmise pendant ces périodes ne sera pas nécessairement réécrite sur Moodle ou autrement.

Les personnes enseignantes ne peuvent garantir une réponse rapide par courriel. À moins qu'il ne s'agisse d'une communication à caractère privé, sensible ou personnel, les personnes étudiantes doivent communiquer avec la personne enseignante sur Teams dans le canal public du cours afin de permettre à d'autres personnes d'y répondre. La personne enseignante pourra corriger la réponse s'il y a lieu.

3 Matériel nécessaire pour l'activité pédagogique

Les personnes étudiantes seront également appelées à utiliser le logiciel Zotero. L'accès à un correcteur tel qu'Antidote est fortement recommandé.

D'autres supports matériels variés seront disponibles sur le site du cours Moodle, dans la section "Fichier" du canal Teams du cours ou via les banques de données de la bibliothèque. Selon l'activité pédagogique, les personnes étudiantes auront à leur disposition des diapositives, des textes ou des références à des sites web, des vidéos et textes qui peuvent être rédigés en anglais.

4 Références

[1] CAIJ - Article 342.1 Code criminel. Library Catalog : secure.livechatinc.com.

[2] CAIJ - Article 342.2 Code criminel. Library Catalog : secure.livechatinc.com.

[3] CAIJ - Définition du méfait à l'égard de données informatiques. Library Catalog : secure.livechatinc.com.

[4] Charte canadienne des droits et libertés. Last Modified : 2020-08-07.

[5] Code criminel.

[6] Loi constitutionnelle de 1867. Last Modified : 2020-08-07.

[7] Loi sur la protection des Canadiens contre la cybercriminalité.

[8] Lois sur la protection des renseignements personnels au Canada (L.R.C. (1985) ch. P-21).

[9] Convention sur la cybercriminalité, November 2004.

[10] Partage des compétences au Canada, May 2016. Page Version ID : 126580541.

[11] Revue de droit criminel : La divulgation électronique de la preuve, May 2018. Library Catalog : Blogger.

[12] Revue de droit criminel : La transcription d'un document électronique est-elle constitutionnellement requise ?, May 2018. Library Catalog : Blogger.

[13] Revue de droit criminel : Un haut degré de littératie informatique n'est pas requis pour lire un DVD, May 2018. Library Catalog : Blogger.

[14] 6 Anti-forensic techniques that every cyber investigator dreads, November 2019. Section : Speed Reading.

[4] https://www.usherbrooke.ca/sciences/fileadmin/sites/sciences/documents/Etudiants_actuels/Informations_academiques_et_reglements/Sciences_Reglement_complementaire.pdf

[5] https://www.usherbrooke.ca/registraire/droits-et-responsabilites/reglement-des-etudes/

[15] A Guide on Top 30 GRC Frameworks in 2019 | Ignyte Assurance, February 2019.

[16] INTERPOL Global Guidelines for Digital Forensics Laboratories, May 2019.

[17] Guidelines to Digital Forensics First Responders_V7.pdf, April 2021.

[18] Introduction à la preuve numérique, March 2022.

[19] Comment se déroule un procès criminel au Canada ? | CliquezJustice.ca, June 2024.

[20] L'article 8 de la Charte canadienne et les fouilles, perquisitions et saisies de matériel informatique, dans Développements récents en droit criminel (2021), February 2024.

[21] Beaudoin, Gérald A. : Partage des pouvoirs. (Référence essentielle pour comprendre la répartition des pouvoirs au Canada).

[22] Canada and Dubois, Alain and Schneider, Philip : *Code criminel et lois connexes annotés 2020*. LexisNexis Canada, 2019. OCLC : 1107492596.

[23] Chan, Gerald and Magotiaux, Susan : *Digital evidence*. Criminal law series. Emond, Toronto, Second edition édition, 2022.

[24] Chan, Gerald J. and Greenspan, Brian H. and Rondinelli, Vincenzo and Magotiaux, Susan : *Digital evidence : a practitioner's handbook*. Criminal law series. Emond Montgomery Publications Limited, Toronto, Canada, 2018. OCLC : on1014233373.

[25] DR. ADEL AZZAM SAQF AL HAIT : Jurisdiction in Cybercrimes : A Comparative Study. *Journal of Law, Policy and Globalization*, 22, 2014.

[26] Faculté de droit, Université Laval : Sources et hiérarchie des normes.

[27] Fairlie, John : What is Law ? *In A brief introduction to law in Canada*, page 3 à 25 de 418. Emond Publishing, 2021. OCLC : 1198993345.

[28] Gottardi, Eric V and MacLellan, Jennifer A and Lacy, Michael and Flumerfelt, Robin and Greenspan, Brian H and Rondinelli, Vincenzo : *Qualifying and Challenging Expert Evidence*. Criminal law series. Emond Publishing, Toronto, ON, 2022. OCLC : 1287926184.

[29] Gouvernement du Canada, Gendarmerie royale du Canada : Cybercriminalité : survol des incidents et des enjeux au Canada | Gendarmerie royale du Canada, December 2014. Last Modified : 2020-06-10.

[30] Government of Canada : Cybercrime in Canada, December 2019. Last Modified : 2019-12-02.

[31] Holt, Thomas J. and Bossler, Adam M. and Seigfried-Spellar, Kathryn C. : *Cybercrime and digital forensics : an introduction*. Routledge, New York, NY, Third edition édition, 2022.

[32] International Organization for Standardization : Principes et processus d'investigation sur incident. Rapport technique 27043, CAN/CSA-ISO/IEC, 2013.

[33] International Organization for Standardization : Vulnerability disclosure. Rapport technique 29147, ISO/IEC, 2014.

[34] International Organization for Standardization : Gouvernance du cadre de risque forensique numérique. Rapport technique 30121, ISO/IEC, 2015.

[35] International Organization for Standardization : Electronic discovery — Part 4 : Technical Readiness (2021). Rapport technique 27050-4 :2021, CAN/CSA-ISO/IEC, 2018.

[36] International Organization for Standardization : Lignes directrices pour l'analyse et l'interprétation des preuves numériques. Rapport technique 27042 :F18, CAN/CSA-ISO/IEC, 2018.

[37] International Organization for Standardization : Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques. Rapport technique 27037 :F18, CAN/CSA-ISO/IEC, 2018.

[38] International Organization for Standardization : Préconisations concernant la garantie d'aptitude à l'emploi et d'adéquation des méthodes d'investigation sur incident. Rapport technique 27041 :F18, CAN/CSA-ISO/IEC, 2018.

[39] International Organization for Standardization : Electronic discovery — Part 1 : Overview and concepts (2021). Rapport technique 27050-1, ISO/IEC, 2019.

[40] International Organization for Standardization : Electronic discovery — Part 3 : Code of practice for electronic discovery (2020). Rapport technique 27050-3 :2020, CSA ISO/IEC, 2020.

[41] James Garrett : Overcoming Reasonable Doubt in Computer Forensics, 2006.

[42] Salhany, Roger E. and Claxton, Edward W. : *The practical guide to evidence and proof in criminal cases*. Emond Montgomery Publications Limited, Toronto, ON, Ninth edition édition, 2022. OCLC : 1287009156.

[43] Shahid Jamal Tubrazy : *The Digital Evidence Forensic Laws in Canada and USA : Theories, Concepts and Practices*. Createspace Independent Publishing Platform, December 2016.

[44] Shavers, Brett and Bair, John : *Hiding behind the keyboard : uncovering covert communication methods with forensic analysis*. Elsevier, Amsterdam : Boston, 2016.

[45] Sheetz, Michael : *Computer Forensics An Essential Guide for Accountants, Lawyers, and Managers*. Wiley, 2015. OCLC : 943787317.

[46] Vincent Gautrais : *La preuve technologique*. LexisNexis, 2e édition édition, 2018. OCLC : 1065108720.

[47] Watkins, Kerry and Rondinelli, Vincenzo and Anderson, Gail S. and Bulmer, Warren : *Evidence and investigation : from the crime scene to the courtroom*. Emond, Toronto, Canada, Second edition édition, 2019. OCLC : 1080211446.

[48] Årnes, André, éditeur. *Digital forensics*. John Wiley & Sons Inc, Hoboken, NJ, 2018.

Faculté des sciences UdS

Délits relatifs aux études

Extrait du règlement des études (Règlement 2575-009)

Sont notamment considérés comme un délit relatif aux études les faits suivants :

a) commettre un plagiat, soit faire passer ou tenter de faire passer pour sien, dans une production évaluée, le travail d'une autre personne, des passages ou idées tirés de l'œuvre d'autrui ou du contenu, de toute forme, généré par un système d'intelligence artificielle (ce qui inclut notamment le fait de ne pas indiquer la source et la référence adéquate);
b) commettre un autoplagiat, soit soumettre, sans autorisation préalable, une même production, en tout ou en partie, à plus d'une activité pédagogique ou dans une même activité pédagogique (notamment en cas de reprise);
c) usurper l'identité d'une autre personne ou procéder à une substitution de personne lors d'une production évaluée ou de toute autre prestation obligatoire;
d) fournir ou obtenir toute forme d'aide non autorisée, qu'elle soit collective ou individuelle (incluant l'assistance provenant d'un système d'intelligence artificielle), pour une production faisant l'objet d'une évaluation;
e) obtenir par vol ou toute autre manœuvre frauduleuse, posséder ou utiliser du matériel non autorisé de toute forme (incluant le matériel numérique et celui généré par un système d'intelligence artificielle) avant ou pendant une production faisant l'objet d'une évaluation;
f) copier, contrefaire ou falsifier un document pour l'évaluation d'une activité pédagogique;
k) posséder ou avoir à sa portée un appareil électronique ou numérique interdit durant une activité d'évaluation;

[...]

Un guide sur l'intégrité intellectuelle vous est rendu disponible par le service des bibliothèques et des archives de l'Université de Sherbrooke, afin de bien comprendre les différents délits et ainsi éviter d'être aux prises avec un dossier disciplinaire et une ou des sanctions.

Les mesures pouvant être imposées à titre de sanctions disciplinaires sont les suivantes :

a) la réprimande simple ou sévère consignée au dossier étudiant pour la période fixée par l'autorité disciplinaire ou à défaut, définitivement. En cas de réprimande fixée pour une période déterminée, la décision rendue demeure au dossier de la personne aux seules fins d'attester de l'existence du délit en cas de récidive;
b) l'obligation de reprendre une production ou une activité pédagogique, dont la note pourra être établie en tenant compte du délit survenu antérieurement;
c) la diminution de la note ou l'attribution de la note E ou 0;

[...]

UDS Faculté des sciences

Balises d'utilisation des outils d'intelligence artificielle générative

Autorisés ou pas dans les situations d'apprentissage et d'évaluation ?

NIVEAU 0	NIVEAU 1	NIVEAU 2	NIVEAU 3	NIVEAU 4
L'utilisation des outils d'intelligence artificielle générative (IAg) est limitée, voire complètement interdite parce que la personne enseignante considère que l'usage de ces outils nuit au développement de compétences essentielles. Ces compétences peuvent être disciplinaires, comme elles peuvent être d'ordre méthodologique, rédactionnel ou informationnel. Considérant que l'utilisation des IAg requiert un esprit critique, il peut s'agir d'une situation d'apprentissage ou d'évaluation sans IAg qui vise à développer celui-ci. Dans ces situations, **la personne étudiante produit le travail**.			L'utilisation prononcée des IAg est permise parce que la personne enseignante considère que les personnes étudiantes sont en mesure d'exercer un esprit critique et sont capables de juger de la qualité des contenus produits par les IAg. Ou encore, l'utilisation est encouragée parce que la situation d'apprentissage ou d'évaluation proposée contribue à développer leur esprit critique. Dans ces situations, l'IAg produit le travail préliminaire, alors que **la personne étudiante s'assure de sa qualité en l'améliorant**.	
				
Utilisation interdite	**Utilisation limitée**	**Utilisation guidée**	**Utilisation balisée**	**Utilisation libre**
Le **NIVEAU 0** signifie que l'**utilisation est interdite**. Ceci signifie que si la personne enseignante a un motif de croire qu'il y a eu l'utilisation d'une IAg dans une situation d'évaluation, elle doit dénoncer les faits auprès de la personne responsable des dossiers disciplinaires universitaires. Il s'agit d'un délit relatif aux études tel que stipulé dans le Règlement des études.	Le **NIVEAU 1 D'UTILISATION** signifie que l'**utilisation est autorisée uniquement pour assister l'apprentissage dans le domaine disciplinaire ou des langues**. Dans ce contexte, la personne étudiante **est tenue de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation peut être considérée comme un délit. Par exemple : Domaine disciplinaire : - S'inspirer - Générer des idées - Explorer un sujet pour mieux le comprendre - Générer du matériel pour apprendre Domaine des langues : - Identifier ses erreurs et se les faire expliquer - Reformuler un texte - Générer un plan pour aider à structurer un texte - Traduire un texte	Le **NIVEAU 2 D'UTILISATION** signifie que l'**utilisation est autorisée pour améliorer un travail produit par la personne étudiante**. Dans ce contexte, la personne étudiante **est tenue de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation est considérée comme un délit. Par exemple : - Analyser des contenus - Obtenir une rétroaction - Évaluer la qualité de son travail à partir de critères - Demander à être confronté relativement à ses idées, à sa démarche - Diriger les processus de résolution de problèmes	Le **NIVEAU 3 D'UTILISATION** signifie que l'**utilisation est autorisée pour produire un travail qui sera amélioré.** Dans ce contexte, la personne étudiante **est tenue de citer selon les normes[1] le contenu généré par l'IAg** ou **de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation est considérée comme un délit. Par exemple : - Résumer ou rédiger des parties d'un texte - Générer un texte ou un modèle d'une production et l'adapter - Réaliser des calculs mathématiques - Produire du code informatique - Résoudre des problèmes complexes - Répondre à une question - Générer des images, ou autres contenus multimédias	Le **NIVEAU 4 D'UTILISATION** signifie qu'**aucune restriction spécifique n'est imposée**. Dans ce contexte, la personne étudiante **est tenue de citer selon les normes[1] le contenu généré par l'IAg** ou **de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation est considérée comme un délit. Ce niveau inclut tout ce qui précède, de l'exploration à la production, ainsi que toute autre tâche particulière jugée complexe.

UDS Faculté des sciences

À considérer avant l'utilisation d'outils d'intelligence artificielles génératives

Si, en tant que personne étudiante envisagez d'utiliser un outil d'intelligence artificielle générative (IAG) lorsque l'évaluation autorise les niveaux 1 à 4 d'utilisation mentionnés précédemment.

Dans ce cas, gardez à l'esprit les éléments clés suivants.

- Vous assumez la responsabilité de tout le contenu produit, avec ou sans IAG, et intégré à votre production.
- Les produits des outils d'IAG peuvent très souvent comporter **des erreurs ou des faussetés** (hallucinations) : on doit donc impérativement valider tout contenu généré par ces outils.
- Dans l'état actuel de la Loi sur le droit d'auteur du Canada, les **productions faites par l'IAG sont du domaine public,** puisque les outils d'IAG ne sont pas reconnus comme des auteurs au sens de la Loi et que les contenus générés ne répondent pas aux critères d'une œuvre protégée, notamment aux critères d'originalité.
- L'entreprise qui fournit le service pourrait émettre certaines exigences dans ses conditions d'utilisation. Comme l'algorithme et le code informatique appartiennent à l'entreprise qui les a développés, nous devons tenir compte de ces conditions. Celles-ci pourraient également fournir des précisions relatives à la **réutilisation des données soumises (confidentialité)**.

Comment déclarer l'utilisation d'outils d'intelligence artificielle générative

Dans l'esprit d'une conduite intègre et responsable, vous devez TOUJOURS mentionner de façon explicite toute utilisation de l'intelligence artificielle, conformément au Règlement des études (9.4.1 Délits relatifs aux études). De plus, à des fins pédagogiques, il est recommandé de toujours intégrer à la production les requêtes, de même que les réponses intégrales générées par les outils d'IAG. Celles-ci pourront être intégrées directement dans le corps du texte ou en note de bas de page. Les réponses longues pourraient être insérées en annexe de votre document ou dans des documents supplémentaires, selon les directives de la personne enseignante.

L'utilisation de ces deux documents s'avèrera utile, ils se trouvent sous licence libre, donc vous pouvez utiliser les tableaux et les adapter selon votre besoin:

1. Modèle de citation : Ce formulaire, à remplir par l'enseignant, donne un exemple aux étudiants de citation de l'IAg dans la réalisation d'un travail évalué ou non.
2. Déclaration d'usage : Ce formulaire, à remplir par les étudiants, doit être remis avec une réalisation afin de déclarer l'usage de l'IAg dans la réalisation, qu'elle soit évaluée ou non.

Référence

La Faculté des sciences tient à remercier le SSF pour la production des documents.

- Cabana, M. et Côté, J.-A. (2024). Balises d'utilisation des outils d'intelligence artificielle générative. Service de soutien à la formation, Université de Sherbrooke. Sous licence CC BY 4.0.
- Cabana, M. et Beaudet, M. (2024). Directives de déclaration de l'utilisation de l'intelligence artificielle générative dans une production étudiante. Service de soutien à la formation, Université de Sherbrooke. Sous licence CC BY 4.0.
- Cabana, M. (2024). Formulaire de déclaration de l'utilisation de l'intelligence artificielle générative dans une production étudiante. Service de soutien à la formation, Université de Sherbrooke. Sous licence CC BY 4.0.