Université de Sherbrooke

Centre de formation en technologie de l'information

INF 802 – Planification et prévention en sécurité des TI

Plan d'activité pédagogique

Hiver 2026

Enseignant	Steve Waterhouse
Courriel :	steve.waterhouse@usherbrooke.ca
Local :	
Téléphone :	+1 450 355-0375
Disponibilités :	L'enseignant est disponible sur l'heure du midi ou en fin de journée par courriel.

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

Horaire Exposé magistral : Mardi 18 h 30 à 21 h 50 salle L1-2633

Description officielle de l'activité pédagogique[1]

Cibles de formation :	Comprendre et mettre en place un processus de gestion des incidents. Gérer des vulnérabilités et appliquer une approche proactive contre les cyberattaques. Établir des métriques d'évaluation de la sécurité.
Contenu :	Introduction au concept d'incident/réaction, à la communication et à l'importance d'avoir un plan préétabli ; gestion des incidents (plan d'action et de communication) ; gestion des mises à jour : pourquoi, comment, outils ; détection et journaux : comment mettre en place une solution efficace, mais aussi comprendre les outils, leur détection par signatures et comportement réseau ou hôte ; suivi et trace d'une intrusion ; gestion de risques : niveaux de service, rapports et métriques pour l'évaluation d'une stratégie de gestion des incidents. Prévention de l'hameçonnage ; logiciel d'extorsion ou rançongiciel (ransomware) ; intervention d'une équipe de sécurité (développeurs et administrateurs de système) ; prévention, réaction et introduction de mesure de désescalades postincident (incident/réaction) ; intervention dans un environnement mobile.
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/inf802

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

Cette activité de formation s'inscrit dans le début du microprogramme. Son positionnement permet à l'étudiant d'acquérir les assises d'une gestion des incidents ainsi que l'identification de vulnérabilité en sécurité. L'activité permet de contextualiser les éléments théoriques dans une mise en application terrain de la sécurité TI, dont :

Introduction au concept d'incident/réaction, à la communication et à l'importance d'avoir un plan préétabli. Gestion des incidents (plan d'action et de communication). Gestion des mises à jour : pourquoi, comment, outils. Détection et journaux : comment mettre en place une solution efficace, mais aussi comprendre les outils, leur détection par signatures et comportement réseau ou hôte. Suivi et trace d'une intrusion. Gestion de risques : niveaux de service, rapports et métriques pour l'évaluation d'une stratégie de gestion des incidents. Prévention de l'hameçonnage. Logiciel d'extorsion ou rançongiciel (ransomware). Intervention d'une équipe de sécurité (développeurs et administrateurs de système). Prévention, réaction et introduction de mesure des escalades post-incidents (incident/réaction). Initiation aux différentes normes sur la sécurité des chaînes d'approvisionnement. Intervention dans un environnement mobile, exploration des notions de vie privée et de la protection des renseignements personnels.

1.2 Cibles de formation spécifiques

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

• maîtriser les tenants et aboutissants de la sécurité informatique contemporaine ;

• maîtriser la nature des surfaces d'attaque exposées par une infrastructure de TI ;

• savoir concevoir, mettre en œuvre et documenter une stratégie efficace pour protéger et défendre ces surfaces d'attaque, en tenant compte d'un budget de ressources donné ;

• pouvoir critiquer une telle stratégie telle que mise en place dans une organisation, de manière à en corriger les faiblesses.

1.3 Contenu détaillé

Thème	Contenu	Nbr. d'heures	Objectifs	Lectures[1]
1	Module 1 : Notions de processus et fonctions informatiques : • Introduction au cours INF 802 et présentation enseignant / étudiants • Fondements de la cybersécurité • Pyramide de sécurité de l'information • Pyramide organisationnelle versus pyramide de la sécurité de l'information • Notions de processus • Quelques définitions conceptuelles • Survol à très haut niveau de COBIT 5 • Survol à très haut niveau d'ITIL • Survol de la norme PCI-DSS v4 • Facteurs clés de succès de l'implantation des référentiels, normes, etc. • Raisons de l'adoption de cadres référentiels, normes, etc. • Survol des systèmes de billetterie • Processus de RFC	3		• COBIT 5 : Un référentiel orienté affaires pour la gouvernance et la gestion des TI de l'entreprise, ISBN 978-1-60420-436-0 ; • ISO 27001 :2018 • TOGAF • SABSA • PCI-DSS version 4 (français) • NIST Framework Documents - Cybersecurity Framework Version 1.1 (https ://www.nist.gov/cyberframe) ; – Version française - Cadre pour l'amélioration de la Cybersécurité des infrastructures critiques https ://nvl-pubs.nist.gov/nistpubs/CSW

Table 1 :

Thème	Contenu	Nbr. d'heures	Objectifs	Lectures[1]
2	Module 2 : Processus de gestion d'incidents : • Définitions conceptuelles • Généralités et quelques statistiques • Processus de gestion d'incidents • Cadre référentiel de gestion d'incidents • selon le NIST-sp 800-61 • Objectifs • Phase de préparation • Phase de détection et analyse • Phase de confinement, éradication et recouvrement • Phase de revue post-incident (désescalades) • Quelques indicateurs (métriques) d'incidents • Quelques bonnes pratiques (si possible) • Exemples de processus génériques de gestion d'incidents • Matrice RACI	6		• NIST SP 800-61 - Computer Security Incident Handling Guide (https ://nvlpubs.nist.gov/nistpubs/61r2.pdf) ;
3	Module 3 : Mesures de performances et notions de vie privée : **Définitions conceptuelles** **Généralités sur les mesures de performance** • Objectifs facilitants COBIT 5 • Quelques métriques de gestion d'incidents selon COBIT 5 • Quelques métriques d'incidents selon le NIST-sp-800-61 • Enjeux • Raisons d'utilisation des tableaux de bord • Tableau de bord • Étapes de réalisation d'un tableau de bord • Cascades d'objectifs COBIT 5 **Notion de vie privée** • Respect de la vie privée • Dimensions du respect de la vie privée • Encadrement vie privée et protection des renseignements personnels (PRP) : USA, ONU, Union Européenne, Canada, et Québec • Atteinte à la vie privée et quelques conséquences rattachées au non-respect de la PRP • Quelques contrôles pouvant aider à réduire les risques d'atteinte à la vie privée	3		

Table 1 :

Thème	Contenu	Nbr. d'heures	Objectifs	Lectures[1]
4	Module 4 : Savoir évaluer et reconnaître les menaces : **Contexte** **Définitions conceptuelles** • Anomalie • Incident de sécurité mineur • Incident de sécurité important • Incident de sécurité critique **Notions d'incident majeur** • Délimitation d'incident majeur dans le cadre du module • Quelques incidents majeurs : ¨ Verglas (1998) ¨ Y2K (1999) ¨ Wannacry / NotPetya (2017) ¨ ARC / Equifax (2017) ¨ Marriott (2018-2020) ¨ Desjardins (2019) ¨ Capital One (2019) • ¨ CrowdStrike (2024) ¨ **Gestion de crise** • Généralités • Quelques contrôles de gestion d'incident majeur • Grandes lignes de gestion de crise selon le NIST-sp 800-61 • Quelques constantes dans la gestion de crise • Se préparer avant la crise • Durant la crise • Réponse à la crise • Post-mortem • Stratégies de communication • Exemple de communication de crise	3		
5	Module 5 – Conformité opérationnelle : • Définitions • Menaces et autres • Anticipation de protection envers la menace • Menaces et exploits • Les acteurs et leurs menaces • Attribution – À qui la faute ? **Travail pratique #2 – Savoir évaluer et reconnaître les menaces**	3		• NIST SP 800-171 Rev 3 – Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations https ://nvlpubs.nist.gov/nistpubs/Special 171r3.pdf • NIST SP-800-53 Rev5 - Security and Privacy Controls for Information Systems and Organizations https ://nvlpubs.nist.gov/nistpubs/Special 53r5.pdf

Table 1 :

Thème	Contenu	Nbr. d'heures	Objectifs	Lectures[1]
6	Module 6 : Notions d'incident majeur et de gestion de crise : • Principes de base du CENOPSEC • Les phases du plan • La phase de conception • La phase de construction • La phase d'exploitation • CENOPSEC local ou impartit • La norme SOC2 • Exemple de SOC visités	6		
7	Module 7 - Processus de gestion des vulnérabilités : • Gestion des risques • Évaluation des menaces et des risques (ÉMR) • Définitions relatives à la gestion des vulnérabilités • Élaboration d'une méthodologie d'évaluation des vulnérabilités • Outils de référence avec lesquels à travailler • Émission du Quizz • Travail pratique#3 – Gestion des vulnérabilités	3		
8	Module 8 - Processus de gestion des mises à jour : • Définition de l'importance du processus des mises à jour • Mises à jour PME • Mises à jour GE • Les exceptions (IoT, ICS/SCADA) • Élaboration d'une méthodologie d'évaluation des mises à jour • Problèmes anticipés • Outils ¨ **Travail pratique#4 – Gestion des mises à jour**	6		
9	Module 9 - Prévention de l'hameçonnage : • Définition de ce qu'est l'hameçonnage • Faits vécus • Prévention de l'hameçonnage • Logiciel d'extorsion ou rançongiciel (ransomware) • Intervention d'une équipe de sécurité (développeurs et administrateurs de système) • Prévention, réaction et introduction de mesure de dés escalades post incident (incident/réaction) ¨**Administration de fin de cours**	6		
10	Travail Pratique No.1 – Gestion d'incidents : • ***Critères d'évaluation*** Le travail devra être d'un **maximum de 5 pages** en prenant soin de citer les références. Un retour global sera fait le jeudi suivant la remise du travail. • ***Notation :*** Note sur 100, 20 % de la note finale • ***Date de remise :*** Le travail est à remettre dans Moodle au plus tard le lundi 26 janvier 2026, 22h30 HNE. Le format à recevoir sera sous PDF avec comme nomenclature : INF802AM-H26-TP1-<nomdefamille.initialeprénom>.pdf	8	Comprendre et mettre en place un processus de gestion des incidents Établir des métriques d'évaluation de la sécurité	

Table 1 :

Thème	Contenu	Nbr. d'heures	Objectifs	Lectures[1]
11	Travail Pratique No.2 – Savoir évaluer et reconnaître les menaces : Le travail devra être d'un **maximum de 5 pages** en prenant soin de citer les références. Un retour global sera fait le jeudi suivant la remise du travail. Note sur 100, 20 % de la note finale Le travail est à remettre dans Moodle au plus tard le lundi 9 février 2026, 22h30 HAE. Le format à recevoir sera sous PDF avec comme nomenclature : INF802AM-H26-TP2-<nomdefamille.initialprénom>.pdf	8	Selon un scénario présenté, appliquer les meilleures pratiques vues en classe en lien avec les références Ceci est un travail individuel	
12	Travail Pratique No.3 – Savoir évaluer et reconnaître les menaces : Le travail au total devra être d'un **maximum de 5 pages** en prenant soin de citer les références. Un retour global sera fait le jeudi suivant la remise du travail. Note sur 100, 20 % de la note finale Le travail est à remettre dans Moodle au plus tard le lundi 23 avril 2026, 22h30 HAE. Le format à recevoir sera sous PDF avec comme nomenclature : INF802AM-H26-TP3-<nomdefamille.initialprénom>.pdf	8	Selon un scénario présenté, appliquer les meilleures pratiques vues en classe en lien avec les références Ceci est un travail individuel	
13	Travail Pratique No.4 - Gestion des vulnérabilités : Le travail devra être d'un **maximum de 5 pages** en prenant soin de citer les références. Un retour global sera fait le jeudi suivant la remise du travail. Note sur 100, 20 % de la note finale Le travail est à remettre dans Moodle au plus tard le lundi 6 avril 2026, 22h30 HAE. Le format à recevoir sera sous PDF avec comme nomenclature : INF802AM-H26-TP4-<nomdefamille.initialprénom>. pdf	8	Selon un scénario présenté, appliquer les meilleures pratiques vues en classe en lien avec les références. Ceci est un travail individuel.	

Table 1 :

Thème	Contenu	Nbr. d'heures	Objectifs	Lectures[1]
14	Quiz : • Comprendre et mettre en place un processus de gestion des incidents • Gérer les vulnérabilités et appliquer une approche proactive contre les cyberattaques • ***Critères d'évaluation*** Chaque quiz est composé de questions à choix de réponses sur les éléments présentés dans le module. • ***Notation :*** Le quiz compte pour 20 % de la note finale. • ***Date de mise en disponibilité :*** 10 mars 2026	1	Un quiz individuel à compléter dans Moodle en 60 minutes les notions des modules 1-6	

[1] Les lectures indiquées ne sont là qu'à titre indicatif. L'enseignant est libre de choisir un autre document de référence

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

Apprentissage par sessions en classe de 3h par semaine

2.2 Calendrier

Semaine	Commençant le	Thème		Devoirs
1	2026-01-05	1		
2	2026-01-12	2		
3	2026-01-19	2 et 10	Date de remise pour le TP#1 = Lundi 26 janvier 2026 - 22h30 HNE	
4	2026-01-26	3		Remise Travail pratique No. 1
5	2026-02-02	4 et 11	Date de remise pour le TP#2 = Lundi 9 janvier 2026 - 22h30 HNE	
6	2026-02-09	5		Remise Travail pratique No. 2
7	2026-02-16	6		
8	2026-02-23			
9	2026-03-02	Relâche		
10	2026-03-09	6 et 14		
11	2026-03-16	7		
12	2026-03-23	8 et 12	Date de remise pour le TP#3 = Lundi 23 mars 2026 - 22h30 HAE	Remise Travail pratique No. 3
13	2026-03-30	9 et 13	Date de remise pour le TP#4 = Lundi 6 avril 2026 - 22h30 HAE	
14	2026-04-06	9		Remise Travail pratique No. 4
15	2026-04-13			
16	2026-04-20	Semaine des examens finals		
17	2026-04-27	Semaine des examens finals		

2.3 Évaluation

Type de l'évaluation	Pondération	Utilisation des IAG[1]
Devoirs (4)	80 %	Limitée
Examen intra	20 %	Interdite

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

Écriture de 4 dissertations d'un maximum de 5 pages sur une mise en situation donnée

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

Devoirs	Sujet	Réception	Remise	Points
Travail pratique No. 1	Analyse de gestion des incidents	2026-01-20	2026-01-26	20
Travail pratique No. 2	Savoir évaluer et reconnaître les menaces	2026-02-03	2026-02-09	20
Travail pratique No. 3	Gestion des vulnérabilités	2026-03-17	2026-03-23	20
Travail pratique No. 4	Gestion des mises à jour	2026-03-31	2026-04-06	20

[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.

3 Matériel nécessaire pour l'activité pédagogique

Les notes seront compilées dans Moodle

[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/

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.