Université de Sherbrooke

Centre de formation en technologie de l'information
INF 806 – Système et réseau

Plan d'activité pédagogique

Hiver 2026

Enseignant	Sofiane Touel
Courriel :	sofiane.touel@usherbrooke.ca
Local :	
Téléphone :	

Disponibilités : Je suis pleinement investi dans votre réussite et demeure à votre entière disposition pour échanger sur le contenu du cours, vos réflexions sur le domaine de la cybersécurité ou votre futur cheminement professionnel.
Modalités de communication :
Courriel : C'est le moyen privilégié pour me joindre. Je m'engage à vous répondre dans un délai minimal de **48 heures ouvrables**.
Rencontres individuelles : Si une discussion plus approfondie s'avère nécessaire (clarification technique, mentorat, suivi de projet), nous pouvons planifier une rencontre virtuelle.
Flexibilité horaire : Afin de m'adapter à vos réalités, les plages horaires de rencontre sont flexibles et peuvent être fixées, selon nos disponibilités mutuelles, durant les heures ouvrables, en soirée ou exceptionnellement le week-end.
Il ne faut pas attendre la veille d'un examen ou d'une remise de projet pour manifester vos interrogations !

Site web du cours : MS Teams

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

---

Description officielle de l'activité pédagogique[1]

[1] https ://www.usherbrooke.ca/admission/fiches-cours/inf806

Cibles de formation :	Connaitre les caractéristiques de l'architecture des composantes des réseaux informatiques dans un contexte de sécurité. Comprendre les principes d'architecture réseau et de sécurité.
Contenu :	Réseau : postes de travail, serveurs, applications Web, SGDBD, routeurs, commutateurs, point d'accès sans fil, pare-feu, serveur mandataire (Proxy), antivirus, courriels, filtrage de contenu, authentification, surveillance réseau. Détection de logiciels malveillants. Services de base en réseautique, virtualisation. Principes d'architecture réseau et de sécurité : OSI, TCP/IP, zonage ou segmentation réseau, flots de trafic, sécurité interzone ; attaque réseau, honeytoken, détection des pivots. Système : bac à sable (sandbox), cuckoosandbox, principes de base. Analyse des cas de type C&C irc, twitter, zeus. Cryptologie.
Crédits	3
Organisation	3 heures d'exposé magistral par semaine 6 heures de travail personnel par semaine
Particularités	Aucune

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

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	Fondements de la cybersécurité : contexte professionnel, menaces courantes et bases techniques : • Panorama du monde du travail en cybersécurité : rôles, responsabilités, attentes du marché • Compétences clés et certifications reconnues en cybersécurité • Rappels fondamentaux en réseaux et systèmes (DNS, HTTP, postes, serveurs) • Introduction aux menaces courantes ciblant les utilisateurs • Phishing : mécanismes, objectifs, impacts organisationnels • Sécurité du courriel : principes généraux et surfaces d'attaque • Introduction aux concepts fondamentaux : confidentialité, intégrité, disponibilité • Notions de menace, vulnérabilité, risque et contrôle de sécurité	3		Révision : • Modèle CIA (Confidentialité, Intégrité, Disponibilité) • Différence menace / vulnérabilité / risque / contrôle • Principes du phishing et de la sécurité du courriel • Concepts SPF, DKIM, DMARC (niveau conceptuel) Préparation séance 2 : • Notions de base sur le chiffrement symétrique et asymétrique • Rôle des certificats numériques • Vue d'ensemble TLS / PKI (ressource d'introduction)

Table 1 :

Thème	Contenu	Nbr. d'heures	Objectifs	Lectures[1]
2	Sujet du projet 1 et Cryptographie appliquée et sécurité des communications : chiffrement, hachage et TLS : • Rappel des concepts vus à la séance précédente • **Sujet du projet 1** • Chiffrement symétrique : principes, usages, limites • Chiffrement asymétrique : clés publiques et privées, cas d'usage • Différence entre chiffrement, hachage et signature numérique • Fonction de hachage : objectifs, propriétés, usages en sécurité • HTTPS et TLS : rôle dans la sécurisation des communications • Compréhension conceptuelle du fonctionnement d'une connexion sécurisée	3		Révision : • Phishing et sécurité courriel • Bases réseaux et systèmes (DNS, HTTP, journaux) • Préparation séance 3 : • Introduction aux vulnérabilités logicielles • Lecture d'introduction sur CVE et NVD • Principes généraux du score CVSS (base, vecteurs, limites)
3	Gestion des vulnérabilités et priorisation du risque : CVE, CVSS et IA en sécurité : • Rappels sur cryptographie et hachage • Définition d'une vulnérabilité logicielle • Cycle de vie d'une vulnérabilité (découverte → publication → correctif) • Base de données CVE et rôle de la NVD • Compréhension détaillée du score CVSS (vecteurs, impacts, sévérité) • Limites du CVSS et importance du contexte organisationnel • Processus de gestion des vulnérabilités : – Inventaire des actifs – Analyse – Priorisation – Remédiation – Validation • Introduction aux usages et risques de l'IA générative en cybersécurité	3		Révision : • Différences entre chiffrement, hachage et signature • Principes TLS et PKI Préparation séance 4 : • Concepts IAM / GIA • RBAC, privilèges, MFA • Principe du moindre privilège • Séparation des tâches

Table 1 :

Thème	Contenu	Nbr. d'heures	Objectifs	Lectures[1]
4	Gestion des identités et des accès (GIA) : contrôle des privilèges et sécurisation des comptes : • Rappel de la démarche de gestion des vulnérabilités • Introduction à la gestion des identités et des accès • Rôles, utilisateurs, groupes et permissions • RBAC : principe et avantages • MFA : facteurs d'authentification et scénarios d'attaque évités • Accès conditionnel : logique et objectifs • PAM : sécurisation des comptes à privilèges • Risques liés aux comptes administrateurs	3		Révision : • CVE, CVSS et processus de vulnérabilité Préparation séance 5 : • Concepts de pare-feu et ACL • Segmentation réseau et DMZ • Différence IDS / IPS (niveau conceptuel)
5	Sécurité des réseaux – Partie 1 : périmètre, filtrage et détection des intrusions : • Rappel sur IAM et comptes à privilèges • Rôle du réseau dans la posture de sécurité • Pare-feu : filtrage, règles, périmètre • Listes de contrôle d'accès (ACL) • IDS vs IPS : objectifs et différences • Filtrage Web et contrôle des flux • Segmentation réseau et réduction de surface d'attaque	3		Révision : • RBAC, MFA, accès conditionnel, PAM Préparation séance 6 : • Principes Zero Trust • VLAN et NAC • Panorama SASE / SSE
6	Présentation du projet 1	3		
7	Sécurité des réseaux – Partie 2 : architectures modernes et approche Zero Trust : • Revenir sur le projet • Principe Zero Trust : ne jamais faire confiance, toujours vérifier • VLAN et segmentation logique • NAC : contrôle d'accès au réseau • Architecture réseau sécurisée moderne • Introduction aux concepts SASE et SSE • Lien entre identité, réseau et posture de sécurité	3		Révision : • Pare-feu, IDS, IPS • Segmentation et filtrage
8	Examen mi-session	3		

Table 1 :

Thème	Contenu	Nbr. d'heures	Objectifs	Lectures[1]
9	Sujet du projet 2 et Sécurité des postes et gestion des points de terminaisons : Endpoints, journaux, SIEM et WAF : • Revenir sur l'examen • **Sujet du projet 2** • Sécurité des postes de travail • EDR : détection et réponse sur les endpoints • SIEM : collecte, corrélation et analyse • WAF : protection applicative • Types de journaux et alertes	3		Préparation séance prochaine : • Responsabilité partagée en cloud • Bases de sécurité cloud • Attaques DDoS (principes)
10	Sécurité infonuagique et résilience : responsabilité partagée, DDoS et SIEM cloud : • Modèle de responsabilité partagée • Spécificités de la sécurité cloud • Sécurité des identités, du réseau et du stockage en cloud • Attaques DDoS : mécanismes et impacts • Positionnement d'un SIEM cloud (ex. Sentinel)	3		Révision séance précédente Préparation séance prochaine : • Cycle de réponse aux incidents • Artefacts forensiques • Principes de collecte et de traçabilité
11	Investigation numérique et exposition externe : forensic, scan passif et renseignement : • Rappel sur sécurité cloud • Cycle de réponse aux incidents • Principes de forensic numérique • Scan passif et collecte d'information • Outils de collecte (ex. Velociraptor) • Exposition externe et moteurs spécialisés (ex. Shodan)	3		Révision séance précédente Préparation séance prochaine : • OWASP Top 10 • Impacts des vulnérabilités applicatives • Bonnes pratiques de mitigation (sans exploitation)
12	Présentation du projet 2	3		
13	Sécurité offensive et défensive des applications et systèmes : OWASP et mitigation : • Retour sur le projet2 • OWASP Top 10 : vue d'ensemble • Types de vulnérabilités applicatives • Impacts techniques et métiers • Approche défensive et mesures de mitigation • Lien entre vulnérabilités, risques et contrôles	3		
14	Evaluation finale	3		

[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

L'enseignement de ce cours repose sur une approche dynamique et appliquée, conçue pour transformer les concepts théoriques en compétences opérationnelles. Chaque séance débute par une présentation magistrale des éléments de compétence, où la théorie est systématiquement illustrée par des exemples concrets, des études de cas réels et des démonstrations techniques. Cette méthode permet d'établir un lien direct et immédiat entre les éléments de sécurité et leur mise en œuvre dans le monde du travail.

Afin de favoriser un apprentissage par l'action, des activités pratiques telles que des laboratoires, des ateliers ou des travaux de groupe sont intégrées aux séances. Pour soutenir votre réussite et respecter l'équilibre de votre charge de travail, la majeure partie des exercices techniques se déroule durant les heures de cours, permettant ainsi un accompagnement personnalisé en temps réel. En complément de ces séances, un temps est spécifiquement alloué à l'extérieur de la classe pour vos lectures préparatoires et la révision des concepts.

Sur le plan technologique, nous explorerons un écosystème varié composé d'outils open source, de versions d'essai professionnelles et de ressources spécifiques fournies par l'institution. L'environnement technologique pourra être enrichi de nouveaux modules ou logiciels selon les opportunités de licences et l'évolution rapide des menaces actuelles. Par souci d'équité et de planification, notez que la totalité des évaluations, incluant les examens et les présentations de projets, se tiendra exclusivement pendant les périodes de cours prévues au calendrier.

Enfin, bien que le plan de cours définisse les grandes orientations de la session, il demeure flexible afin de mieux s'adapter à votre réalité. Les thèmes et le rythme de progression pourront être ajustés selon le niveau d'avancement du groupe, vos acquis préalables et la disponibilité des ressources techniques. Cette agilité pédagogique assure que le contenu demeure pertinent et aligné sur vos besoins de formation ainsi que sur les standards de l'industrie de la cybersécurité.

2.2 Calendrier

Semaine	Commençant le	Thème	
1	2026-01-05	1	
2	2026-01-12	2	
3	2026-01-19	3	
4	2026-01-26	4	
5	2026-02-02	5	
6	2026-02-09	6	
7	2026-02-16	7	
8	2026-02-23	8	
9	2026-03-02	Relâche	
10	2026-03-09	9	
11	2026-03-16	10	
12	2026-03-23	11	
13	2026-03-30	12	
14	2026-04-06	Lundi de Pâques	
15	2026-04-13	13	
16	2026-04-20	Semaine des examens finals	Pas d'examen
17	2026-04-27	Semaine des examens finals	

2.3 Évaluation

Type de l'évaluation	Pondération	Utilisation des IAG[1]
Projet 1	25 %	Libre
Projet 2	25 %	Libre
Examen intra	25 %	Libre
Examen final	25 %	Libre

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

Les évaluations et projets visent à mesurer l'atteinte des compétences ciblées, telles que définies dans le plan de cours. Celles-ci prennent la forme de livrables pratiques, produits en classe (avec possibilité de finalisation à la maison pour les projets), à remettre aux dates prévues dans le plan d'évaluation.

Les critères généraux de correction sont les suivants :

•Conformité aux consignes fournies ;
•Justesse et pertinence des réponses ;
•Fonctionnalité et efficacité des solutions produites ;
•Respect des standards et bonnes pratiques présentées en cours ;
•Fonctionnement opérationnel des composants ;
•Clarté et lisibilité des interfaces ou rendus visuels ;
•Qualité des choix techniques (structures, outils, méthodes) ;
•Logique, lisibilité et simplicité de la démarche ou du code (le cas échéant) ;
•Validation rigoureuse des résultats attendus.
•La collaboration si applicable ;
•Lisibilité et clarté du contenu, qu'il soit technique ou visuel ;
•Qualité de la programmation ou de la configuration (le cas échéant) ;
•Respect de la propriété intellectuelle : toute source externe, outil IA ou modèle utilisé doit être explicitement cité ;
•Respect des droits d'auteur : il est strictement interdit de reproduire des portions de code ou de documentation sans attribution claire ;
•En cas de présentation orale, la clarté de la communication, la maîtrise du sujet et la structuration seront évaluées ;
•Pour les livrables numériques, les métadonnées et l'historique de création peuvent être analysés afin de vérifier l'authenticité du travail.

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

Les dates de remise des travaux seront indiquées sur les énoncés.

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

Matériel : Ordinateur avec internet, caméra, micro et casque.

Logiciel : Teams et machine virtuelle

[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/

[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.