Université du Québec en Outaouais **Département d'informatique et d'ingénierie**

Sigle : CYB1063 Gr. 01
Titre : Communication et leadership en cybersécurité
Session : Hiver 2026 / Horaire et local
Professeur : Hamou-Lhadj, Abdel

1. Description du cours paraissant à l'annuaire :

Objectifs

Au terme de ce cours, l'étudiant(e) sera prêt(e) à jouer un rôle central dans une organisation en utilisant des techniques de communication efficaces afin de traduire dans un langage d'affaire les enjeux de cybersécurité.

Contenu

Analyse de risque au niveau organisationnel. Engagement des parties prenantes, techniques de négociation et présentation efficace. Conversion du risque technique en risque organisationnel. Escalade de l'information en réponse aux incidents, échange d'information rapide et efficace (breffage), contrôle et dissémination de l'information et relation avec les médias. Rédaction de rapports techniques en cybersécurité. Transfert de connaissances et formation des utilisateurs aux pratiques responsables en cybersécurité. Résolution de problèmes de communication en cybersécurité issus du monde réel.

Descriptif - Annuaire

2. Objectifs spécifiques du cours :

- Comprendre l'importance de la cybersécurité dans les organisations et les enjeux stratégiques associés
- Comprendre les fondements de la communication et du leadership dans le domaine de la cybersécurité
- Intégrer les enjeux de la cybersécurité dans le fonctionnement d'une organisation et acquérir des compétences en matière d'analyse, de pensée critique et de prise de décision
- Développer des compétences de leadership, de communication et de travail en équipe sur des problématiques de cybersécurité

3. Stratégies pédagogiques :

La démarche pédagogique du cours encourage vivement la participation des étudiant(e)s au développement de leurs propres savoirs en communication et leadership en cybersécurité dans des organisations diverses.

Les méthodes pédagogiques privilégiées pour ce cours incluent lectures, réflexions et activités en équipe, études de cas, présentations magistrales et travaux d'analyse en groupe.

Notes :

- Ce cours se donnera en mode non-présentiel. Les séances de cours se donneront sur la plateforme ZOOM.
- Pendant toute la durée des séances de cours, il est fortement recommandé que les étudiant(e)s soient visibles sur caméra afin de faciliter les interactions et discussions en groupe.
- Il n'y a pas de séances de TD/TP programmées pour ce cours.

Règles de bienséance :

Les règles de fonctionnement dans ce cours seront disponibles sur Moodle et discutées lors de la 1ère séance du cours.

4. Heures de disponibilité ou modalités pour rendez-vous :

Pour obtenir un rendez-vous, envoyez un courriel à : abdel.hamou-lhadj@uqo.ca

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	▪ Introduction au cours ▪ Concepts clés en gestion des organisations	16 janvier 2026
2	▪ Importance des enjeux de la cybersécurité dans les organisations modernes	23 janvier 2026
3	▪ Intégration de la cybersécurité dans la vision stratégique des organisations	30 janvier 2026
4	▪ Contribution de la cybersécurité à la gestion de risques dans les organisations	06 février 2026
5	▪ Rôle stratégique du responsable de la cybersécurité dans les organisations ➔ **Devoir #1 à rendre**	13 février 2026
6	▪ Fondements du leadership dans les problématiques de la cybersécurité	20 février 2026
7	▪ Mise en application du leadership dans des situations de crise en cybersécurité	27 février 2026
8	***Semaine d'études***	06 mars 2026
9	▪ Fondements de la communication dans le domaine de la cybersécurité	13 mars 2026
10	▪ Développement d'un plan directeur de communication pour la cybersécurité ➔ **Devoir #2 à rendre**	20 mars 2026
11	▪ Déploiement d'un plan directeur de communication dans une organisation	27 mars 2026
14	***Jour férié (Vendredi Saint)***	03 avril 2026
12	▪ Gestion de la résistance au changement et les pratiques non désirables	10 avril 2026
13	➔ **Présentation des travaux de groupe et documents à rendre**	17 avril 2026
15	➔ **Examen final**	24 avril 2026

6. Évaluation du cours :

- Deux devoirs individuels – 30%
- Un travail de groupe (avec évaluation des pairs) – 30%
- Un examen final – 40%

Note : L'examen final se déroulera conformément au calendrier et modalités des examens finaux de l'université pour la session d'hiver 2026.

7. Politiques départementales et institutionnelles :

- Politique du département d'informatique et d'ingénierie relative à la tenue des examens
- Note sur le plagiat et sur la fraude
- Politique relative à la qualité de l'expression française écrite chez les étudiants et les étudiantes de premier cycle à l'UQO
- Absence aux examens : cadre de gestion, demande de reprise d'examen (formulaire)

Tolérance ZÉRO en matière de violence à caractère sexuel.

Le Bureau d'intervention et de prévention en matière de harcèlement (BIPH) a pour mission d'accueillir, soutenir et guider toute personne vivant une situation de harcèlement, de discrimination ou de violence à caractère sexuel. Le BIPH oriente ses actions afin de prévenir les violences à caractère sexuel pour que nous puissions étudier, travailler et s'épanouir dans un milieu sain et sécuritaire.
Vous vivez ou êtes une personne témoin d'une situation de violence à caractère sexuel ? Vous êtes une personne membre de la communauté étudiante ou une personne membre du personnel, autant à Gatineau qu'à Ripon et St-Jérôme, l'équipe du BIPH est là pour vous, sans jugement et en toute confidentialité.
Ensemble, participons à une culture de respect.
Pour de plus amples renseignements consultez UQO.ca/biph ou écrivez-nous au Biph@uqo.ca

8. Principales références :

- Il n'y a pas de livre obligatoire pour ce cours.
- La liste des lectures obligatoires pour ce cours inclut les références suivantes :
  - Le rôle de la cybersécurité et de la sécurité des données dans l'économie numérique
  - Leadership de la cybersécurité
  - Cybersecurity and Corporate Governance
  - Anticiper et gérer sa communication de crise cyber
  - Stratégie de cybersécurité à Banque Canada 2022-2024
  - Meilleures pratiques en matière de cybersécurité municipale
  - Guide de sensibilisation à la sécurité de l'information
  - 20 Questions que les administrateurs devraient poser sur la cybersécurité
  - 11 Strategies of a World-Class Cybersecurity Operations Center
- La liste ci-dessus pourrait être enrichie par quelques lectures supplémentaires sur Moodle, en fonction des centres d'intérêt des étudiant(e)s.

9. Page Web du cours :

https://moodle.uqo.ca