Sigle : CYB1063 Gr. 01
Titre : Communication et leadership en cybersécurité
Session : Hiver 2023 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 étudiants 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.

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

Pour obtenir un rendez-vous, envoyez un courriel à : abdelkrim.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	13 janvier
2	• Importance des enjeux de la cybersécurité dans les organisations modernes	20 janvier
3	• Intégration de la cybersécurité dans la vision stratégique des organisations	27 janvier

4	• Contribution de la cybersécurité à la gestion de risques dans les organisations	3 février
5	• Rôle stratégique du responsable de la cybersécurité dans les organisations	10 février
6	• Fondements du leadership dans les problématiques de la cybersécurité	17 février
7	• Mise en application du leadership dans des situations de crise en cybersécurité	24 février
8	• Fondements de la communication dans le domaine de la cybersécurité	3 mars
9	• Semaine d'études	5-10 mars
10	• Développement d'un plan directeur de communication pour la cybersécurité	17 mars
11	• Déploiement du plan directeur de communication dans une organisation	24 mars
12	• Gestion de la résistance au changement et des pratiques non désirables	31 mars
13	• Férié (Vendredi de Pâques)	7 avril
14	• Présentation des travaux de groupe	14 avril
15	• Examen final en classe	21 avril

6. Évaluation du cours :

- Deux travaux individuels – 30%
- Un travail de groupe – 40%
- Un examen final – 30%

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)

La communauté universitaire s'engage à lutter contre les inconduites, le harcèlement et les violences à caractère sexuel. Dénonçons toute forme de violence.
Ensemble, accomplissons un pas de plus en complétant la formation obligatoire en ligne : "La banalisation des violences à caractère sexuel".

uqo.ca/bimi/formation-obligatoire

Pour de plus amples renseignements consultez :

bimi@uqo.ca

UQO BUREAU D'INTERVENTION EN MATIÈRE D'INCONDUITE

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 complète des lectures sera disponible sur Moodle.

9. Page Web du cours :

https://moodle.uqo.ca

10. Règles de bienséance :

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