Code de conduite

École Cybersécurité

Version 1
Juillet 2021

Directives générales

Nous nous attendons à ce que tou(te)s les participant(e)s à l'École Cybersécurité reconnaissent et adhèrent à ce code de conduite. Le terme "participant(e)s" inclut chaque personne présente, ainsi que les organisateurs(-trices), formateurs(-trices), commanditaires, bénévoles, et autres invité(e)s présent(e)s pendant les formations. Nous demandons la coopération de chaque participant(e) afin de nous aider à assurer un environnement sécuritaire pour chacun(e).

Ce code de conduite n'est pas un document légal, mais plutôt une déclaration d'intention concernant le genre d'espace que nous souhaitons créer à l'École Cybersécurité. Les exemples énumérés ci-dessous ne sont pas exhaustifs, mais illustrent bien certains comportements que nous jugeons désalignés avec les valeurs de l'organisme.

Les valeurs de l'École Cybersécurité et le comportement attendu

L'École Cybersécurité se dévoue à fournir un espace positif et sécuritaire pour tou(te)s, et ce, peu importe leur identité de genre, orientation sexuelle, invalidité, apparence physique, taille corporelle, race, religion, âge, statut économique, niveau d'éducation, ou bien leur choix de logiciel d'exploitation, d'éditeur de texte, ou préférence de langage script. En particulier, l'École Cybersécurité priorise la diversité, et s'efforce de devenir un endroit où les membres de groupes démographiques historiquement sous-représentés dans la communauté de sécurité de l'information peuvent s'épanouir.

Soyez amical(e) et accueillant(e)

L'École Cybersécurité est gérée par des bénévoles et animée par des professionnel(le)s en sécurité qui dépensent un nombre incalculable d'heures de leur temps libre afin de créer des formations intéressantes et uniques pour tou(te)s.

Soyez patient(e) et constructif(-ive)

Veuillez garder en tête que nous nous réunissons pour apprendre et partager nos connaissances dans une atmosphère agréable. Toutefois, nous ne partageons pas tous les mêmes compétences, parcours, ou langue maternelle. La communication efficace

nécessite un effort: réfléchissez sur la manière dont vos paroles seront reçues, et évitez de présumer les expériences des autres.

Soyez respectueux(-euse) et collaboratif(-ive)

En particulier, respectez les opinions divergentes ainsi que les différences personnelles. Les organisateurs(-trices), concepteurs(-trices) des défis, et les formateurs(-trices) de l'École Cybersécurité sont tou(te)s des bénévoles qui ont investi beaucoup de temps et d'énergie afin de préparer l'évènement. Si vous pensez trouver des erreurs dans les formations, n'oubliez pas la bonne foi de nos bénévoles.

Politique de comportements inacceptables

Envers les humains

Nous nous attendons que les participant(e)s s'abstiennent de se comporter de manière irrespectueuse, perturbatrice, et illégale autant sur les plateformes en lignes telles que Moodle et Discord que lors des événements en formule présentielle.Il est attendu que toutes et tous se comportent avec respect les un(e)s envers les autres en tout temps.

La liste qui suit est une liste non exhaustive de comportements jugés inacceptables à l'École Cybersécurité:

- Publier des informations sensibles, personnelles, ou privées concernant n'importe quel(le) participant(e) sans son consentement explicite.
- Publier du matériel intimidant, harcelant, abusif, discriminatoire, dérogatoire, ou humiliant.
- Se comporter de manière intimidante, harcelante, abusive, discriminatoire, dérogatoire, ou humiliante envers n'importe quel(le) participant(e).
- Perturber les présentations ou les labs.
- Formuler des commentaires offensifs, discriminatoires, ou inappropriés concernant le sexe, l'identité et l'expression du genre, l'orientation sexuelle, l'invalidité, la santé mentale, la neuroatypicité, l'apparence physique l'origine ethnique, ou la religion.

- Formuler des commentaires offensifs, discriminatoires, ou inappropriés concernant les choix de vie, incluant ceux relatifs à la nourriture, la santé, le style parental, les médicaments, et l'emploi.
- Adopter un comportement sexuel gratuit, indésirable et hors sujet.
- Remarques de nature sexuelle dans l'absence du consentement affirmatif et explicite de chaque participant(e). .
- Le harcèlement, la traque furtive, les menaces de violence ou l'incitation à la violence contre n'importe quelle personne ou groupe.
- Porter ou présenter des slogans ou symboles offensifs ou discriminatoires.
- Le contact social inapproprié. Par exemple: si vous persistez de parler avec quelqu'un(e) qui a indiqué qu'il ou elle ne veut pas parler avec vous.
- N'importe quel comportement qui met en danger la sécurité physique ou l'intégrité corporelle d'autrui.

Nos formateurs(-trices), bénévoles et commanditaires sont soumis à la même politique que les participant(e)s. En particulier, nos formateurs-trices ne doivent pas utiliser ou faire référence à du matériel discriminatoire ou de nature sexuelle dans leurs présentations et ateliers.

Envers les actifs informationnels

L'École Cybersécurité exploite une infrastructure informatique. Appart de l'infrastructure mise en place pour l'examen CTF, toute usage des installations en place (site web, Moodle, etc.) pour pirater ou commettre un acte illégal est strictement défendu.

Signaler un comportement inacceptable

Si vous subissez un comportement inacceptable ou du harcèlement, ou que vous remarquez que quelqu'un(e) est l'objet d'un comportement inacceptable ou du harcèlement, ou que vous avez d'autres préoccupations, veuillez avertir un(e) organisateur(-trice) de l'École Cybersécurité aussitôt que possible. Tout compte rendu est considéré comme confidentiel par défaut. Si la personne qui donne son rapport veut participer dans la résolution de la situation, l'équipe de l'École Cybersécurité ne prendra aucune décision sur la situation sans leur consentement.

Si la personne qui s'est comportée de manière inacceptable ou harcelante est membre de l'équipe organisatrice l'École Cybersécurité, cette personne sera tenue, par la politique de l'École Cybersécurité, de se retirer de participer dans le traitement de la plainte.

Les membres du conseil d'administration de l'École Cybersécurité seront disponibles pour aider les participant(e)s pour fournir un accompagnement, ou pour assister d'une autre manière les personnes ciblées par un comportement inacceptable ou harcelant pour qu'elles se sentent en sécurité pendant une formation.

Vous pouvez signaler en personne pendant une formation tout comportement indésirable à n'importe quel(le) organisateur(-trice), ou envoyer un courriel à l'adresse fournie au bas de cette page, qui est vérifiée régulièrement..

Les conséquences du comportement inacceptable

Vous êtes tenu(e)s de vous conformer immédiatement à toute demande de la part de l'équipe de l'École Cybersécurité. Si un(e) participant(e) est reconnu(e) s'être comporté(e) de manière inacceptable, l'équipe de l'École Cybersécurité prendra toutes mesures estimées appropriées, qui peut aller jusqu'à l'expulsion de la formation et de tous les évènements de l'École Cybersécurité futurs sans avertissement ou remboursement. Les mesures appropriées ont pour objectif d'atténuer le tort qui s'est produit, de résoudre le conflit le cas échéant, et de protéger les participants et participantes de la répétition du préjudice. Par exemple, une réponse appropriée pourrait exiger qu'une personne demande pardon, rembourse le matériel endommagé, ou quitte une formation.

S'il y a un désaccord concernant la définition d'un comportement inacceptable ou regardant l'interprétation de cette politique, contactez-nous en utilisant l'information au bas de cette page.

Politique sur la publication responsable de vulnérabilités

L'École Cybersécurité accorde une grande priorité aux questions de sécurité et est consciente de l'importance de la protection de la confidentialité de l'information à travers

une politique sur la publication responsable. Conformément à cette politique, toute vulnérabilité sécuritaire trouvée doit être divulguée.

Information à signaler:

Pour que nous puissions analyser la vulnérabilité correctement, veuillez nous fournir un rapport de vulnérabilité complet incluant les informations suivantes: Système ou programme vulnérable: décrire où est survenue la vulnérabilité et tous les paramètres/informations reliés;

- Le type de vulnérabilité;
- Étapes pour le reproduire: la démarche à suivre pour reproduire le problème;
- Des captures d'écran qui montrent l'attaque;
- Scénario d'attaque: un exemple de scénario peut aider à prouver le risque et encourager une résolution du problème plus rapide.

Une fois que nous avons reçu un rapport de vulnérabilité complet, nous suivrons la démarche suivante:

- Nous vous demanderons de garder confidentielles toutes les communications relatives à la vulnérabilité pendant au moins 30 jours.
- Nous mènerons une enquête et vérifierons la vulnérabilité.
- Nous remédierons au problème le cas échéant et publierons une mise à jour pour corriger le logiciel.
- Les normes de publication responsable indiquent qu'après avoir signalé le problème en privé, nous aurons 30 jours pour résoudre la vulnérabilité avant d'en aviser le public, dans le cas où aviser le public est nécessaire.

Politique sur le droit d'auteur

Tous les participant(e)s doivent respecter la Loi canadienne sur le droit d'auteur qui protège les artistes, formateurs(-trices), donneurs d'ateliers de l'École Cybersécurité, ainsi que les propriétaires de logiciels et leurs éditeurs. Une utilisation des ressources imprimées ou numériques mises en place par l'École Cybersécurité qui enfreint la Loi sur le droit d'auteur est strictement interdite. Ceci s'applique à toutes formes de

productions médiatiques peu importe son format (textuel, images, vidéos, bandes sonores) et inclut sans s'y limiter l'ensemble du contenu des formations.

Intégrité intellectuelle

Chaque participant(e) doit contribuer activement à la réussite de sa formation et assumer personnellement toutes les tâches exigées dans le cheminement de la formation suivie.

Les actes qui constituent un plagiat, une fraude ou un copiage :

- L'exécution par une autre personne d'un examen, d'un travail ou d'une activité
- L'appropriation et la copie partielle ou totale des œuvres ou des idées d'autrui en les faisant passer pour les siennes
- l'obtention par vol, manoeuvre ou corruption ou toute autre moyen illicite, de questions ou de réponses d'examen
- la sollicitation, l'offre ou l'échange d'information pendant un examen
- Le recours à tout aide non autorisée à l'occasion d'un examen

Tout acte de plagiat, de tricherie ou de copiage entraînera une exclusion immédiate et définitive de l'École Cybersécurité. La personne qui en est l'objet ne pourra plus être admise ou réadmise à une formation ou activité de l'École Cybersécurité. Elle ne pourra plus obtenir de certification de l'École Cybersécurité et elle se verra retirer l'ensemble des certifications de l'École Cybersécurité obtenues avant et après l'acte.

Si vous êtes témoin d'une infraction, veuillez contacter l'équipe de direction de l'École Cybersécurité.