CHARTE CYBER ETHIC

Cyber ETHIC s'engage à la mise en œuvre d'une ligne de conduite éthique, responsable et humaine dans l'ensemble de ses activités.

Cyber ETHIC s'engage dans ce sens au respect des valeurs et principes du Code Of Ethics and Professional Conduct de l'Association for Computing Machinery (ACM) dont les éléments sont repris ci-après.

En complément, Cyber ETHIC respecte les engagements aux principes suivants :

Intégrité

Cyber ETHIC s'engage à proposer des services et solutions dans le respect des lois et réglementations en vigueur.

Cyber ETHIC s'interdit d'utiliser tous moyens qui seraient contraires aux lois ou à la bonne morale, sans limitation au périmètre de ses activités.

Elle s'assure de ne pas être soumise à un quelconque conflit d'intérêt dans la réalisation de ses missions qui serait de nature à mettre en cause son indépendance et son objectivité sur les conseils auprès des structures qu'elle accompagne.

Loyauté

Cyber ETHIC s'engage à rechercher en tout temps et tous lieux l'intérêt suprême de l'organisation qu'elle accompagne. Cela implique de proposer uniquement les services et solutions dont l'organisation a besoin, en s'assurant de la cohérence avec les ressources qu'elle est capable de mobiliser et les compétences internes permettant d'assurer une réponse durable à sa problématique.

Elle s'engage à ne s'impliquer dans aucune activité qui serait de nature à porter préjudice, directement ou indirectement, à ses collaborateurs, ses clients ou sa réputation.

Bienveillance

Cyber ETHIC s'engage à agir en toute bienveillance et à accompagner les organisations sans jugement et dans un objectif de construction et d'élévation de la maturité cybersécurité de l'organisation et de son personnel.

Dans cet objectif, elle met en œuvre les moyens les plus adaptés, fait preuve de pédagogie et d'écoute.

Partage

Cyber ETHIC s'engage à partager la connaissance en matière de cybersécurité dès qu'il lui en ait donné l'occasion. Cela se traduit par la participation à des interventions lors des événements du domaine, des sollicitations non commerciales auprès de la population, des étudiants ou d'associations.

Elle s'engage également à alerter et communiquer sur les menaces liées à la cybersécurité par tous moyens à sa convenance dans l'intérêt général et sans ambition mercantile première.

Cyber ETHIC participe activement aux instances de concertation en matière de cybersécurité pour faire grandir et diffuser le savoir en la matière auprès du plus large public.

CHARTE CYBER ETHIC

Entraide

Cyber ETHIC prône des valeurs d'entraide, dans ce sens elle s'engage dans l'accompagnement des plus jeunes, l'égalité des chances et l'inclusion de tous.

Elle mène des actions concrètes visant à promouvoir ces principes et les diffuser.

Elle apporte son conseil ponctuel aux organisations pour l'orientation de leur réflexion en matière de sécurité des informations.

CHARTE CYBER ETHIC

Code d’éthique et de conduite professionnelle de l’ACM

Préambule

Les actions des professionnels de l'informatique changent le monde. Pour agir de manière responsable, ils doivent réfléchir aux impacts plus larges de leur travail, en soutenant constamment le bien public. Le Code d'éthique et de conduite professionnelle d'ACM (« le Code ») exprime la conscience de la profession.

Le Code est conçu pour inspirer et guider la conduite éthique de tous les professionnels de l'informatique, y compris les praticiens actuels et futurs, les instructeurs, les étudiants, les influenceurs et toute personne utilisant la technologie informatique de manière percutante. De plus, le Code sert de base à des mesures correctives en cas de violations. Le Code comprend des principes formulés sous forme de déclarations de responsabilité, fondées sur l'idée que le bien public est toujours la considération primordiale. Chaque principe est complété par des lignes directrices qui fournissent des explications pour aider les professionnels de l'informatique à comprendre et à appliquer le principe.

La section 1 décrit les principes éthiques fondamentaux qui constituent la base du reste du Code. La section 2 aborde des considérations supplémentaires et plus spécifiques sur la responsabilité professionnelle. La section 3 guide les personnes qui jouent un rôle de leadership, que ce soit sur le lieu de travail ou à titre professionnel bénévole. L'engagement envers une conduite éthique est requis de la part de chaque membre de l'ACM, membre de l'ACM SIG, lauréat du prix ACM et lauréat du prix ACM SIG. Les principes impliquant le respect du Code sont énoncés dans la section 4.

Le Code dans son ensemble s'intéresse à la manière dont les principes éthiques fondamentaux s'appliquent à la conduite d'un professionnel de l'informatique. Le Code n’est pas un algorithme permettant de résoudre des problèmes éthiques ; il sert plutôt de base à une prise de décision éthique. Lorsqu'il réfléchit à un problème particulier, un professionnel de l'informatique peut constater que plusieurs principes doivent être pris en compte et que différents principes auront une pertinence différente pour le problème. La meilleure façon de répondre aux questions liées à ce type de problèmes consiste à examiner attentivement les principes éthiques fondamentaux, en sachant que le bien public est la considération primordiale. La profession informatique dans son ensemble en profite lorsque le processus de prise de décision éthique est responsable et transparent envers toutes les parties prenantes. Des discussions ouvertes sur les questions éthiques favorisent cette responsabilité et cette transparence.

CHARTE CYBER ETHIC

1. PRINCIPES ÉTHIQUES GÉNÉRAUX.

Un professionnel de l'informatique devrait...

1.1 Contribuer à la société et au bien-être humain, en reconnaissant que tous sont parties prenantes de l'informatique.

Ce principe, qui concerne la qualité de vie de toutes les personnes, affirme une obligation des professionnels de l'informatique, tant individuellement que collectivement, d'utiliser leurs compétences au profit de la société, de ses membres et de l'environnement qui les entoure. Cette obligation inclut la promotion des droits humains fondamentaux et la protection du droit de chaque individu à l'autonomie. L'un des objectifs essentiels des professionnels de l'informatique est de minimiser les conséquences négatives de l'informatique, notamment les menaces pour la santé, la sûreté, la sécurité personnelle et la vie privée. Lorsque les intérêts de plusieurs groupes sont en conflit, les besoins des moins favorisés devraient recevoir une attention et une priorité accrues.

Les professionnels de l'informatique devraient se demander si les résultats de leurs efforts respecteront la diversité, seront utilisés de manière socialement responsable, répondront aux besoins sociaux et seront largement accessibles. Ils sont encouragés à contribuer activement à la société en s'engageant dans un travail bénévole qui profite au bien public.

Outre un environnement social sûr, le bien-être humain nécessite un environnement naturel sûr. Par conséquent, les professionnels de l'informatique devraient promouvoir la durabilité environnementale tant au niveau local que mondial.

1.2 Éviter les dommages.

Dans ce document, « préjudice » désigne des conséquences négatives, surtout lorsque ces conséquences sont importantes et injustes. Les exemples de préjudice comprennent les blessures physiques ou mentales injustifiées, la destruction ou la divulgation injustifiée d'informations et les dommages injustifiés à la propriété, à la réputation et à l'environnement. Cette liste n'est pas exhaustive.

Des actions bien intentionnées, y compris celles visant à accomplir des tâches assignées, peuvent entraîner un préjudice. Lorsque ce préjudice n'est pas intentionnel, les responsables sont tenus de réparer ou d'atténuer le préjudice autant que possible. Éviter les préjudices commence par un examen attentif des impacts potentiels sur toutes les personnes touchées par les décisions. Lorsque le préjudice fait intentionnellement partie du système, les responsables sont tenus de veiller à ce que le préjudice soit éthiquement justifié. Dans les deux cas, assurez-vous que tous les dommages sont minimisés.

Pour minimiser la possibilité de nuire indirectement ou involontairement à autrui, les professionnels de l'informatique doivent suivre les meilleures pratiques généralement acceptées, à moins qu'il n'existe une raison éthique impérieuse de faire autrement. De plus, les conséquences de l'agrégation des données et les propriétés émergentes des systèmes doivent être soigneusement analysées. Les personnes impliquées dans les systèmes omniprésents ou d'infrastructure devraient également prendre en compte le principe 3.7.

Un professionnel de l'informatique a l'obligation supplémentaire de signaler tout signe de risque système susceptible d'entraîner un préjudice. Si les dirigeants n'agissent pas pour réduire ou atténuer ces risques, il peut être nécessaire de « dénoncer » pour réduire les dommages potentiels. Cependant, une déclaration erronée des risques peut en soi être préjudiciable. Avant de signaler les risques, un professionnel de l'informatique doit évaluer soigneusement les aspects pertinents de la situation.

1.3 Soyez honnête et digne de confiance.

L'honnêteté est un élément essentiel de la fiabilité. Un professionnel de l'informatique doit être transparent et fournir une divulgation complète de toutes les capacités, limitations et problèmes potentiels pertinents du système aux parties concernées. Faire des déclarations délibérément fausses ou trompeuses, fabriquer ou falsifier des données, offrir ou accepter des pots-de-vin et toute autre conduite malhonnête constituent des violations du Code.

Les professionnels de l'informatique doivent être honnêtes quant à leurs qualifications et quant à toute limitation de leur compétence pour accomplir une tâche. Les professionnels de l'informatique doivent être francs sur toute circonstance qui pourrait conduire à des conflits d'intérêts réels ou perçus ou qui tendrait à porter atteinte à l'indépendance de leur jugement. De plus, les engagements doivent être honorés.

Les professionnels de l'informatique ne doivent pas déformer les politiques ou procédures d'une organisation et ne doivent pas parler au nom d'une organisation à moins d'y être autorisés.

1.4 Soyez juste et prenez des mesures pour ne pas faire de discrimination.

Les valeurs d'égalité, de tolérance, de respect d'autrui et de justice régissent ce principe. L'équité exige que même des processus décisionnels minutieux offrent une certaine possibilité de réparation des griefs.

Les professionnels de l'informatique devraient favoriser une participation équitable de tous, y compris ceux des groupes sous-représentés. La discrimination préjudiciable fondée sur l'âge, la couleur, le handicap, l'origine ethnique, la situation familiale, l'identité de genre, l'appartenance à un syndicat, le statut militaire, la nationalité, la race, la religion ou les convictions, le sexe, l'orientation sexuelle ou tout autre facteur inapproprié constitue une violation explicite du code. Le harcèlement, y compris le harcèlement sexuel, l'intimidation et autres abus de pouvoir et d'autorité, est une forme de discrimination qui, entre autres préjudices, limite l'accès équitable aux espaces virtuels et physiques où ce harcèlement a lieu.

L'utilisation de l'information et de la technologie peut créer de nouvelles inégalités ou renforcer celles qui existent déjà. Les technologies et les pratiques doivent être aussi inclusives et accessibles que possible et les professionnels de l'informatique doivent prendre des mesures pour éviter de créer des systèmes ou des technologies qui privent les gens de leurs droits ou les oppriment. Le fait de ne pas concevoir l'inclusion et l'accessibilité peut constituer une discrimination injuste.

1.5 Respecter le travail requis pour produire de nouvelles idées, inventions, œuvres créatives et artefacts informatiques.

Développer de nouvelles idées, inventions, œuvres créatives et artefacts informatiques crée de la valeur pour la société, et ceux qui déploient cet effort doivent s'attendre à tirer une valeur de leur travail. Les professionnels de l'informatique devraient donc créditer les créateurs d'idées, d'inventions, d'œuvres et d'artefacts, et respecter les droits d'auteur, les brevets, les secrets commerciaux, les accords de licence et autres méthodes de protection des œuvres des auteurs.

La coutume et la loi reconnaissent que certaines exceptions au contrôle d'un créateur sur une œuvre sont nécessaires pour le bien public. Les professionnels de l'informatique ne doivent pas s'opposer indûment à des utilisations raisonnables de leurs œuvres intellectuelles. Les efforts visant à aider les autres en consacrant du temps et de l'énergie à des projets qui aident la société illustrent un aspect positif de ce principe. Ces efforts incluent des logiciels et des travaux gratuits et open source placée dans le domaine public. Les professionnels de l'informatique ne devraient pas revendiquer la propriété privée du travail qu'eux-mêmes ou d'autres ont partagé en tant que ressources publiques.

1.6 Respecter la vie privée.

La responsabilité du respect de la vie privée s'applique de manière particulièrement profonde aux professionnels de l'informatique. La technologie permet la collecte, la surveillance et l'échange de renseignements personnels rapidement, à peu de frais et souvent à l'insu des personnes concernées. Par conséquent, un professionnel de l'informatique doit se familiariser avec les différentes définitions et formes de confidentialité et comprendre les droits et responsabilités associés à la collecte et à l'utilisation d'informations personnelles.

Les professionnels de l'informatique ne doivent utiliser les informations personnelles qu'à des fins légitimes et sans violer les droits des individus et des groupes. Cela nécessite de prendre des précautions pour empêcher la réidentification de données anonymisées ou la collecte de données non autorisées, de garantir l'exactitude des données, de comprendre leur provenance et de les protéger contre tout accès non autorisé et toute divulgation accidentelle. Les professionnels de l'informatique doivent établir des politiques et des procédures transparentes qui permettent aux individus de comprendre quelles données sont collectées et comment elles sont utilisées, de donner leur consentement éclairé pour la collecte automatique de données et d'examiner, d'obtenir, de corriger les inexactitudes et de supprimer leurs données personnelles.

Seule la quantité minimale d'informations personnelles nécessaire doit être collectée dans un système. Les périodes de conservation et d'élimination de ces informations doivent être clairement définies, appliquées et communiquées aux personnes concernées. Les renseignements personnels recueillis dans un but précis ne doivent pas être utilisés à d'autres fins sans le consentement de la personne. Les collections de données fusionnées peuvent compromettre les fonctionnalités de confidentialité présentes dans les collections d'origine. Par conséquent, les professionnels de l'informatique doivent veiller particulièrement à la confidentialité lors de la fusion de collections de données.

1.7 Respecter la confidentialité.

Les professionnels de l'informatique se voient souvent confier des informations confidentielles telles que des secrets commerciaux, des données clients, des stratégies commerciales non publiques, des informations financières, des données de recherche, des articles scientifiques préalables à la publication et des demandes de brevet. Les professionnels de l'informatique doivent protéger la confidentialité, sauf dans les cas où cela prouve une violation de la loi, des règlements organisationnels ou du Code. Dans ces cas, la nature ou le contenu de ces informations ne doivent être divulgués qu'aux autorités compétentes. Un professionnel de l'informatique doit réfléchir attentivement à la question de savoir si ces divulgations sont conformes au Code.

2. RESPONSABILITÉS PROFESSIONNELLES.

Un professionnel de l'informatique devrait...

2.1 S'efforcer d'atteindre une qualité élevée tant dans les processus que dans les produits du travail professionnel.

Les professionnels de l'informatique devraient insister et soutenir un travail de haute qualité de leur part et de celui de leurs collègues. La dignité des employeurs, des employés, des collègues, des clients, des utilisateurs et de toute autre personne touchée directement ou indirectement par les travaux doit être respectée tout au long du processus. Les professionnels de l'informatique doivent respecter le droit des personnes impliquées à une communication transparente sur le projet. Les professionnels doivent être conscients de toutes les conséquences négatives graves pouvant résulter d'un travail de mauvaise qualité affectant toute partie prenante et doivent résister aux incitations à négliger cette responsabilité.

2.2 Maintenir des normes élevées de compétence professionnelle, de conduite et de pratique éthique.

L'informatique de haute qualité dépend d'individus et d'équipes qui assument la responsabilité personnelle et collective d'acquérir et de maintenir des compétences professionnelles. La compétence professionnelle commence par des connaissances techniques et par la conscience du contexte social dans lequel leur travail peut être déployé. La compétence professionnelle nécessite également des compétences en communication, en analyse réflexive, ainsi qu'en reconnaissance et en gestion des défis éthiques. Le perfectionnement des compétences doit être un processus continu et peut inclure des études indépendantes, la participation à des conférences ou des séminaires et d'autres formations informelles ou formelles. Les organisations professionnelles et les employeurs devraient encourager et faciliter ces activités.

2.3 Connaître et respecter les règles en vigueur relatives au travail professionnel.

Les « règles » incluent ici les lois et réglementations locales, régionales, nationales et internationales, ainsi que toutes les politiques et procédures des organisations auxquelles appartient le professionnel. Les professionnels de l'informatique doivent respecter ces règles, à moins qu'il n'existe une justification éthique impérieuse pour agir autrement. Les règles jugées contraires à l'éthique devraient être contestées. Une règle peut être contraire à l'éthique lorsqu'elle repose sur un fondement moral inadéquat ou qu'elle cause un préjudice reconnaissable. Un professionnel de l'informatique devrait envisager de contester la règle via les canaux existants avant de la violer. Un professionnel de l'informatique qui décide d'enfreindre une règle parce qu'elle est contraire à l'éthique ou pour toute autre raison doit considérer les conséquences potentielles et accepter la responsabilité de cet acte.

2.4 Accepter et fournir un examen professionnel approprié.

Un travail professionnel de haute qualité en informatique dépend d'un examen professionnel à toutes les étapes. Chaque fois que cela est approprié, les professionnels de l'informatique doivent rechercher et utiliser l'examen par les pairs et les parties prenantes. Les professionnels de l'informatique doivent également fournir des critiques constructives et critiques sur le travail des autres.

2.5 Donner des évaluations complètes et approfondies des systèmes informatiques et de leurs impacts, y compris une analyse des risques possibles.

Les professionnels de l'informatique occupent une position de confiance et ont donc la responsabilité particulière de fournir des évaluations et des témoignages objectifs et crédibles aux employeurs, aux employés, aux clients, aux utilisateurs et au public. Les professionnels de l'informatique doivent s'efforcer d'être perspicaces, minutieux et objectifs lorsqu'ils évaluent, recommandent et présentent des descriptions de systèmes et des alternatives. Des précautions extraordinaires doivent être prises pour identifier et atténuer les risques potentiels dans les systèmes d'apprentissage automatique. Un système pour lequel les risques futurs ne peuvent pas être prédits de manière fiable nécessite une réévaluation fréquente des risques à mesure que le système évolue dans son utilisation, sinon il ne devrait pas être déployé. Tout problème pouvant entraîner un risque majeur doit être signalé aux parties appropriées.

2.6 Effectuer des travaux uniquement dans les domaines de compétence.

Un professionnel de l'informatique est chargé d'évaluer les missions de travail potentielles. Cela comprend l'évaluation de la faisabilité et de l'opportunité du travail, ainsi que le jugement quant à savoir si le travail assigné relève des domaines de compétence du professionnel. Si, à tout moment avant ou pendant la mission, le professionnel constate un manque d'expertise nécessaire, il doit le divulguer à l'employeur ou au client. Le client ou l'employeur peut décider de poursuivre la mission avec le professionnel après un délai supplémentaire pour acquérir les compétences nécessaires, de poursuivre la mission avec une autre personne possédant l'expertise requise ou d'y renoncer. Le jugement éthique d'un professionnel de l'informatique devrait être le guide final pour décider s'il doit travailler sur cette mission.

2.7 Favoriser la sensibilisation et la compréhension du public à l'informatique, aux technologies connexes et à leurs conséquences.

En fonction du contexte et des capacités de chacun, les professionnels de l'informatique devraient partager leurs connaissances techniques avec le public, favoriser la sensibilisation à l'informatique et encourager la compréhension de l'informatique. Ces communications avec le public doivent être claires, respectueuses et accueillantes. Les questions importantes comprennent les impacts des systèmes informatiques, leurs limites, leurs vulnérabilités et les opportunités qu'ils présentent. De plus, un professionnel de l'informatique doit traiter avec respect les informations inexactes ou trompeuses liées à l'informatique.

2.8 Accéder aux ressources informatiques et de communication uniquement lorsque cela est autorisé ou lorsque l'intérêt public l'exige.

Les individus et les organisations ont le droit de restreindre l'accès à leurs systèmes et données tant que les restrictions sont conformes aux autres principes du Code. Par conséquent, les professionnels de l'informatique ne devraient pas accéder au système informatique, aux logiciels ou aux données d'autrui sans avoir une conviction raisonnable qu'une telle action serait autorisée ou une conviction impérieuse qu'elle est conforme au bien public. Un système étant accessible au public ne constitue pas en soi un motif suffisant pour impliquer une autorisation. Dans des circonstances exceptionnelles, un professionnel de l'informatique peut utiliser un accès non autorisé pour perturber ou inhiber le fonctionnement de systèmes malveillants ; des précautions extraordinaires doivent être prises dans ces cas-là pour éviter de nuire à autrui.

2.9 Concevoir et mettre en œuvre des systèmes robustes et sécurisés.

Les atteintes à la sécurité informatique causent des dommages. Une sécurité robuste doit être une considération primordiale lors de la conception et de la mise en œuvre de systèmes. Les professionnels de l'informatique doivent faire preuve de diligence raisonnable pour garantir que le système fonctionne comme prévu et prendre les mesures appropriées pour protéger les ressources contre toute utilisation abusive, modification et déni de service accidentels et intentionnels. Étant donné que les menaces peuvent apparaître et changer après le déploiement d'un système, les professionnels de l'informatique doivent intégrer des techniques et des politiques d'atténuation, telles que la surveillance, l'application de correctifs et le reporting des vulnérabilités. Les professionnels de l'informatique doivent également prendre des mesures pour garantir que les parties concernées par les violations de données soient informées en temps opportun et de manière claire, en fournissant des conseils et des mesures correctives appropriées.

Pour garantir que le système atteint son objectif prévu, les fonctionnalités de sécurité doivent être conçues pour être aussi intuitives et faciles à utiliser que possible. Les professionnels de l'informatique devraient décourager les mesures de sécurité qui prêtent à confusion, sont inappropriées en fonction de la situation ou empêchent une utilisation légitime.

Dans les cas où une mauvaise utilisation ou un préjudice est prévisible ou inévitable, la meilleure option peut être de ne pas mettre en œuvre le système.

3. PRINCIPES DE LEADERSHIP PROFESSIONNEL.

Le leadership peut soit être une désignation formelle, soit découler de manière informelle d'une influence exercée sur autrui. Dans cette section, « leader » désigne tout membre d'une organisation ou d'un groupe qui a de l'influence, des responsabilités éducatives ou des responsabilités de gestion. Bien que ces principes s'appliquent à tous les professionnels de l'informatique, les dirigeants ont la responsabilité accrue de les respecter et de les promouvoir, tant au sein de leur organisation que par l'intermédiaire de celle-ci.

Un professionnel de l'informatique, en particulier celui qui agit en tant que leader, devrait...

3.1 Veiller à ce que le bien public soit la préoccupation centrale lors de tout travail informatique professionnel.

Les personnes, y compris les utilisateurs, les clients, les collègues et les autres personnes concernées directement ou indirectement, doivent toujours être au centre des préoccupations en matière d'informatique. Le bien public doit toujours être une considération explicite lors de l'évaluation des tâches associées à la recherche, à l'analyse des besoins, à la conception, à la mise en œuvre, aux tests, à la validation, au déploiement, à la maintenance, au retrait et à l'élimination. Les professionnels de l'informatique doivent garder cette concentration, quelles que soient les méthodologies ou techniques qu'ils utilisent dans leur pratique.

3.2 Articuler, encourager l'acceptation et évaluer l'accomplissement des responsabilités sociales par les membres de l'organisation ou du groupe.

Les organisations et groupes techniques affectent la société au sens large et leurs dirigeants doivent accepter les responsabilités qui y sont associées. Les organisations, grâce à des procédures et des attitudes orientées vers la qualité, la transparence et le bien-être de la société, réduisent les dommages causés au public et sensibilisent à l'influence de la technologie dans nos vies. Par conséquent, les dirigeants devraient encourager la pleine participation des professionnels de l'informatique à l'accomplissement des responsabilités sociales pertinentes et décourager les tendances à agir autrement.

3.3 Gérer le personnel et les ressources pour améliorer la qualité de vie au travail.

Les dirigeants doivent veiller à améliorer, et non à dégrader, la qualité de la vie au travail. Les dirigeants doivent tenir compte du développement personnel et professionnel, des exigences d'accessibilité, de la sécurité physique, du bien-être psychologique et de la dignité humaine de tous les travailleurs. Des normes ergonomiques appropriées pour les relations homme-machine doivent être utilisées sur le lieu de travail.

3.4 Articuler, appliquer et soutenir des politiques et des processus qui reflètent les principes du Code.

Les dirigeants doivent mettre en œuvre des politiques organisationnelles clairement définies et conformes au Code et les communiquer efficacement aux parties prenantes concernées. En outre, les dirigeants doivent encourager et récompenser le respect de ces politiques et prendre les mesures appropriées en cas de violation de ces politiques. Concevoir ou mettre en œuvre des processus qui, délibérément ou par négligence, violent ou tendent à permettre la violation des principes du Code est éthiquement inacceptable.

3.5 Créer des opportunités pour les membres de l'organisation ou du groupe de se développer en tant que professionnels.

Les opportunités de formation sont essentielles pour tous les membres de l'organisation et du groupe. Les dirigeants devraient veiller à ce que des opportunités soient offertes aux professionnels de l'informatique pour les aider à améliorer leurs connaissances et leurs compétences professionnelles, dans la pratique de l'éthique et dans leurs spécialités techniques. Ces opportunités devraient inclure des expériences qui familiarisent les professionnels de l'informatique avec les conséquences et les limites de l'utilisation des systèmes. Les professionnels de l'informatique doivent être pleinement conscients des dangers des approches trop simplistes, de l'improbabilité d'anticiper toutes les conditions de fonctionnement possibles, du caractère inévitable des erreurs logicielles, des interactions des systèmes et de leurs contextes, ainsi que d'autres questions liées à la complexité de leur métier, et pleinement assumer les responsabilités du travail qu'ils accomplissent.

3.6 Soyez prudent lors de la modification ou du retrait des systèmes.

Les changements d'interface, la suppression de fonctionnalités ou encore les mises à jour logicielles ont un impact sur la productivité des utilisateurs et la qualité de leur travail. Les dirigeants doivent faire preuve de prudence lorsqu'ils modifient ou interrompent le support des fonctionnalités du système dont les gens dépendent encore. Les dirigeants devraient étudier en profondeur des alternatives viables à la suppression du support d'un système existant. Si ces alternatives sont trop risquées ou peu pratiques, le développeur doit aider les parties prenantes à migrer en douceur du système vers une alternative. Les utilisateurs doivent être informés des risques liés à l'utilisation continue du système non pris en charge bien avant la fin du support. Les professionnels de l'informatique doivent aider les utilisateurs de systèmes à surveiller la viabilité opérationnelle de leurs systèmes informatiques et les aider à comprendre qu'il peut être nécessaire de remplacer en temps opportun des fonctionnalités inappropriées ou obsolètes ou des systèmes entiers.

3.7 Reconnaître et accorder une attention particulière aux systèmes qui s'intègrent à l'infrastructure de la société.

Même les systèmes informatiques les plus simples ont le potentiel d'avoir un impact sur tous les aspects de la société lorsqu'ils sont intégrés aux activités quotidiennes telles que le commerce, les voyages, le gouvernement, les soins de santé et l'éducation. Lorsque les organisations et les groupes développent des systèmes qui deviennent une partie importante de l'infrastructure de la société, leurs dirigeants ont la responsabilité supplémentaire d'être de bons gestionnaires de ces systèmes. Une partie de cette gestion nécessite l'établissement de politiques garantissant un accès équitable au système, y compris pour ceux qui ont pu être exclus. Cette gestion nécessite également que les professionnels de l'informatique surveillent le niveau d'intégration de leurs systèmes dans l'infrastructure de la société. À mesure que le niveau d'adoption change, les responsabilités éthiques de l'organisation ou du groupe sont susceptibles de changer également. Une surveillance continue de la manière dont la société utilise un système permettra à l'organisation ou au groupe de rester cohérent avec ses obligations éthiques décrites dans le Code. Lorsqu'il n'existe pas de normes de diligence appropriées, les professionnels de l'informatique ont le devoir de veiller à leur mise en place.

4. RESPECT DU CODE.

Un professionnel de l'informatique devrait...

4.1 Soutenir, promouvoir et respecter les principes du Code.

L'avenir de l'informatique dépend à la fois de l'excellence technique et éthique. Les professionnels de l'informatique doivent adhérer aux principes du Code et contribuer à leur amélioration. Les professionnels de l'informatique qui reconnaissent des violations du Code doivent prendre des mesures pour résoudre les problèmes éthiques qu'ils reconnaissent, notamment, lorsque cela est raisonnable, en exprimant leurs inquiétudes à la ou aux personnes soupçonnées d'enfreindre le Code.

4.2 Traiter les violations du Code comme incompatibles avec l'adhésion à l'ACM.

Chaque membre de l'ACM doit encourager et soutenir l'adhésion de tous les professionnels de l'informatique, quelle que soit leur adhésion à l'ACM. Les membres de l'ACM qui reconnaissent une violation du Code devraient envisager de signaler la violation à l'ACM, ce qui peut entraîner des mesures correctives, comme spécifié dans la politique d'application du Code d'éthique et de conduite professionnelle de l'ACM.

Le code a été traduit de l'original via Google Traduction puis vérifié et corrigé par Cyber ETHIC, néanmoins des coquilles ou erreurs de syntaxe ont pu échapper à notre vigilance. N'hésitez pas à nous faire part de toutes remarques via le formulaire Contact.