# Projet: PREMIER Code d'éthique et de déontologie

Les membres des équipes d'intervention et de sécurité en cas d'incident (ci-après désignées sous le terme "Équipes") ont accès à de nombreux systèmes et sources d'information numériques. Leurs actions peuvent changer la donne à l'échelle mondiale. En tant que membre de cette profession, un membre d'Équipe se doit d'assumer ses responsabilités à l'égard des parties prenantes internes, des autres professionnels de la sécurité et de la société au sens large. Il doit être également responsable vis-à-vis de son propre bien-être.

Le présent Code entend inspirer et guider le comportement éthique de tous les membres d'Équipes, y compris les praticiens, les instructeurs, les étudiants et les influenceurs actuels ou futurs, ainsi que tous ceux qui utilisent la technologie informatique pour générer un impact. Le Code énonce des principes formulés sous forme de déclarations de responsabilité qui reposent sur le postulat que le bien public est toujours la considération principale. Chaque principe s'accompagne de directives qui fournissent des explications aux informaticiens pour les aider à mieux comprendre et appliquer le principe en question.

Les responsabilités sont présentées ci-après, sans toutefois être classées par ordre d'importance. Elles ne doivent pas être considérées comme des exigences absolues, mais plutôt comme des préconisations ou recommandations au titre de la norme IETF RFC2119:

> "il peut y avoir des raisons valables dans des circonstances particulières de ne pas tenir compte de l'énoncé considéré, mais il convient cependant de bien mesurer et examiner toutes les implications d'un tel choix."

Pour de plus amples informations sur la manière de gérer les éventuels dilemmes, se reporter à l'Annexe A.

## Devoir de fiabilité

La confiance est à la base de nombreuses relations entre les Équipes. Elle est souvent requise avant de pouvoir procéder à des échanges importants d'informations. La communauté FIRST est bâtie sur la confiance et pourra continuer à opérer ainsi uniquement s'il existe un niveau de confiance raisonnable entre les Équipes.

La fiabilité signifie que les membres d'Équipes devraient uniquement: 1) prendre des engagements qu'ils peuvent tenir; 2) adopter un comportement prévisible vis-à-vis des autres membres d'Équipes (par exemple, respecter la norme TLP); et 3) préserver la relation de confiance qu'ils entretiennent avec les autres membres d'Équipes.

La relation de confiance devrait être implicite et initialement transitive, c'est-à-dire instaurée dès le premier contact (*Trust on First Use – TOFU*), et les Équipes bénéficiant de la confiance d'autres Équipes devraient être automatiquement considérées comme dignes de confiance.

## Devoir de divulgation coordonnée des vulnérabilités

Les membres d'Équipes apprenant l'existence d'une vulnérabilité, devraient respecter les principes de divulgation coordonnée des vulnérabilités en coopérant avec les parties prenantes pour remédier à la faille de sécurité et minimiser les préjudices liés à la divulgation. Les parties prenantes peuvent inclure, sans toutefois s'y limiter, la personne signalant la vulnérabilité, le ou les fournisseurs affectés, les coordonnateurs, les défenseurs, et les clients, partenaires et utilisateurs en aval.

Les membres d'Équipes devraient collaborer avec les parties prenantes compétentes pour convenir d'échéances et d'attentes claires relatives à la divulgation de l'information, tout en fournissant suffisamment de détails pour permettre aux utilisateurs d'évaluer les risques et prendre des mesures défensives réalistes.

## Devoir de confidentialité

Les membres d'Équipes ont la responsabilité de respecter la confidentialité lorsque la situation l'exige. La demande de confidentialité concernant certaines informations peut être formulée de manière explicite, par exemple, par le biais du Traffic Light Protocol (TLP ou Protocole par feux de signalisation). Les membres d'Équipes doivent respecter ce type de demande dans la mesure du possible. S'il est impossible de préserver la confidentialité d'une information, en raison, notamment, de conflits avec les lois locales, les exigences contractuelles ou le devoir d'informer, les membres d'Équipes devraient informer immédiatement le propriétaire de l'information de ce conflit.

Certains devoirs de confidentialité s'appuient sur des lois, des règlements ou le droit coutumier. Si, au cours d'une intervention en cas d'incident, certaines parties sont tenues ou concernées par le devoir de confidentialité en raison de telles considérations, elles doivent s'atteler à faire connaître explicitement ces attentes de façon anticipée. Toutes les parties doivent alors répondre à cette attente en honorant, dans la mesure du possible, la demande explicite de préserver la confidentialité de l'information.

## Devoir de confirmation de reception

Les Équipes reçoivent des informations de nombreuses sources distinctes, à savoir des chercheurs, des clients, d'autres Équipes, des entités gouvernementales, etc. Les membres d'Équipes devraient répondre aux demandes en temps voulu, même s'ils ne font qu'accuser réception de la requête dans un premier temps. Le cas échéant, les membres d'Équipes devraient se fixer des objectifs de délai avant la prochaine réponse.

## Devoir d'autorisation

Les membres d'Équipes ont le droit (et un besoin légitime) de connaître leurs domaines de responsabilité, afin d'agir uniquement dans le cadre des systèmes pour lesquels ils bénéficient d'une autorisation d'accès. Les membres d'Équipes doivent prendre conscience de l'impact de

leurs actions sur les parties prenantes et s'assurer qu'ils ne causent pas de dommage supplémentaire en exécutant leurs fonctions. Les conséquences éventuelles de ces actions devraient être expliquées aux parties prenantes concernées. Dans la mesure du possible, les parties prenantes devraient être consultées avant que des modifications soient apportées à leurs systèmes.

## Devoir d'informer

Les membres d'Équipes devraient considérer qu'il est de leur devoir d'informer les parties prenantes des menaces et des risques de sécurité en cours. Lorsque les membres d'Équipes ont en leur possession des informations pouvant mettre à mal ou, au contraire améliorer, la sûreté et la sécurité, ils ont le devoir d'informer les parties prenantes concernées, ou d'autres intervenants d'appui, tout en tenant dûment compte des règles de confidentialité, des lois et réglementations sur la protection de la vie privée et d'autres obligations.

## Devoir de respecter les droits humains

Les membres d'Équipes devraient être conscients que leurs actions peuvent entraver les droits fondamentaux de certaines personnes, du fait du partage d'informations, des éventuels préjugés guidant leurs actions ou de la violation des droits de propriété. Les membres d'Équipes ont accès à un large éventail d'informations personnelles, sensibles et confidentielles au cours du traitement des incidents. Ces informations doivent être traitées de manière à respecter les droits humains.

Au cours du traitement des incidents, les responsables de la riposte ne devraient pas agir de façon biaisée et devraient s'atteler à éliminer tout parti pris de leurs processus et de leur prise de décisions, que le traitement soit le fait des intervenants ou de certains algorithmes intégrés.

Dans le cadre de ce principe, la notion de "propriété" (Déclaration universelle des droits de l'homme: article 17) englobe les actifs incorporels, tels que la propriété intellectuelle, ainsi que les idées et concepts en général, qu'ils soient légalement protégés (par exemple, brevetés) ou non.

## Devoir de veiller à la santé de l'équipe

Les Équipes ont la responsabilité de poursuivre la prestation des services en honorant leurs engagements auprès des parties prenantes. La responsabilité englobe par là même la préservation de la santé physique et émotionnelle de l'Équipe.

Afin de respecter les membres qui composent l'Équipe et de maintenir un niveau de service adéquat sur le long terme, une Équipe doit s'efforcer de maintenir un environnement de travail sain, sûr et positif qui soutienne la santé physique et émotionnelle de (tous) ses membres. Pour répondre à une situation de crise, les opérations "normales" devraient prendre en charge la santé émotionnelle et diminuer le niveau de stress.

## Devoir de renforcer les capacités de l'équipe

La gestion des incidents est un sujet en perpétuelle évolution que les membres d'Équipes devraient étudier continuellement. Une Équipe devrait fournir à ses membres des ressources

leur permettant d'acquérir des connaissances technologiques et scientifiques dans leur(s) domaine(s) de responsabilité, de les appliquer et de les approfondir. Les crédits de formation CPE/CEU peuvent faciliter cette mise à niveau; de simples exercices de conformité ne sont, quant à eux, pas suffisants pour honorer cette responsabilité. Une Équipe devrait maintenir des infrastructures technologiques suffisantes pour soutenir ses services, et prendre des mesures adéquates pour protéger ces infrastructures de l'ingérence de parties extérieures.

## Devoir de promouvoir une collecte des données responsible

La collecte de données est nécessaire à l'intervention en cas d'incident, mais un équilibre doit être trouvé entre l'objectif de l'intervention en cas d'incident et le respect des données des parties prenantes.

Lors d'une investigation, la quantité d'informations devant être collectées est susceptible de varier. Au cours de l'intervention en cas d'incident, les membres d'Équipes devraient adapter les données collectées à l'évolution des besoins.

Les données n'étant pas directement pertinentes pour l'événement en question ou sa résolution devraient ne pas être prises en compte dans les rapports.

Les données collectées et extraites doivent être traitées dans le respect des lois en vigueur et de la vie privée des utilisateurs. Une permission devrait être obtenue avant de collecter et traiter des données sous la supervision d'un propriétaire des données. Les lois et réglementations en vigueur concernant le traitement des données devraient être respectées.

Les données pouvant aider d'autres Équipes d'intervention affectées à d'autres incidents devraient leur être transmises, de préférence dans une version expurgée. Les informations confidentielles et propriétaires ne devraient être transmises qu'une fois dûment protégées.

Avant de partager des données avec des tiers dans un but d'atténuation, les risques devraient être évalués par rapport aux bénéfices. Les données devraient être partagées uniquement lorsque les bénéfices l'emportent nettement sur les risques. Les données sensibles devraient être stockées de manière à pouvoir les supprimer facilement après la clôture d'un incident. Les données collectées devraient être supprimées en toute sécurité, conformément aux politiques de conservation des données.

## Devoir de reconnaissance des frontières juridictionnelles

Les membres d'Équipes devraient reconnaître et respecter les frontières juridictionnelles, les droits légaux, les règlements et les autorités compétentes régissant les missions des parties impliquées dans les activités relatives à l'intervention en cas d'incident.

Les lois, réglementations et autres mécanismes légaux, tels que ceux relatifs à la protection de la vie privée ou aux notifications en cas de violation des données, peuvent varier entre les différentes juridictions impliquées. Des frontières juridictionnelles peuvent donc être subordonnées à la zone géographique des parties impliquées, telles que leur pays ou leur domicile, ainsi qu'à d'autres facteurs. Même au sein d'un même pays, les lois et réglementations peuvent différer d'une circonscription à une autre (par exemple, entre les différents États des États-Unis) ou selon les entreprises, secteurs ou sous-secteurs nationaux (par exemple, soins de santé, services financiers, équipements publics). Il est possible que les équipes d'intervention en cas d'incident informatique (CSIRT) nationales aient défini des responsabilités ou désigné des autorités pour les activités impliquant des parties prenantes dans leur propre juridiction, et qu'elles aient collaboré avec d'autres entités compétentes dans les juridictions transfrontalières ou qu'elles leur aient transmis des informations ou missions.

Les membres d'Équipes devraient être informés des principales problématiques affectant les juridictions impliquées, y compris, sans toutefois s'y limiter, la réglementation relative à la confidentialité des données ou les exigences de notification en cas de violation des données. La cybersécurité et les lois et réglementations sur la protection de la vie privée évoluent et sont constamment mises à jour à l'échelle mondiale. Il est donc recommandé de consulter un conseiller juridique aguerri pour être guidé lorsque les problématiques couvrent différentes sphères juridictionnelles.

## Devoir de raisonnement fondé sur des données probantes

Les Équipes doivent appuyer leurs opérations sur des données vérifiables. Lors du partage d'informations, telles que des indicateurs de compromission ou des descriptions d'incident, les membres d'Équipes devraient fournir, en toute transparence, des données probantes et des indications sur leur portée. À défaut de pouvoir les produire, les raisons justifiant le non-partage devraient être indiquées.

Les membres d'Équipes devraient s'abstenir de répandre des rumeurs. Toute donnée relevant d'une hypothèse devrait être clairement indiquée comme telle.

La transparence des données probantes et des processus de raisonnement est capitale, même dans le cas de partage automatisé, concernant par exemple, de larges volumes d'informations. Dans ce cas, une description précise et intelligible du processus d'extraction des données devrait être fournie.

# Annexe A

## Gestion des dilemmes

Les membres d'Équipes peuvent être régulièrement confrontés à des situations dans lesquelles aucune action ne semble répondre à l'ensemble des principes éthiques. Dans de tels cas, un choix doit être arrêté quant aux principes à prioriser. Les responsables de la gestion de l'incident sont alors encouragés à identifier d'une part, les parties prenantes potentiellement affectées par les actions mises en œuvre et d'autre part, les circonstances dans lesquelles elles sont ainsi affectées, de préférence dans le cadre d'une discussion avec un collègue. En règle générale, la solution limitant le plus possible l'infraction au présent Code doit être choisie. Il se peut que cela soit impossible, en raison notamment de pressions extérieures. Il est alors recommandé de poursuivre l'action, tout en mentionnant la présence d'un dilemme éthique, éventuellement contesté.