CODE D'ETHIQUE DES MÉTIERS DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

SOMMAIRE

I - PRÉAMBULE

V3. Janvier 1991

Le Code d'Ethique des métiers de la Sécurité des Systèmes d'Information a été élaboré par une commission spécialisée du Clusif.

Ce texte, dans sa version originale, a été approuvé par l'Assemblée Générale du Clusif du 19 décembre 1990, qui a en outre décidé :

- Que tout membre actif du Clusif devait se conformer au présent Code d'Ethique. Le non respect des règles d'éthique définies dans le présent Code constitue un motif d'exclusion du Clusif.
- Que le présent texte doit recevoir une diffusion aussi large que possible aussi bien dans la profession qu'auprès des entreprises utilisatrices de l'informatique, et qu'il est recommandé à tous les professionnels de la Sécurité des Systèmes d'Information de s'y conformer strictement.
- Qu'il est en outre recommandé à tout professionnel et à toute entreprise intervenant comme offreur de produit ou service de Sécurité des Systèmes d'Information d'annexer les dispositions du présent Code d'Ethique aux contrats qu'elle engage avec ses clients, aussi bien qu'à toute entreprise cliente d'exiger cette pratique de la part de son fournisseur.
- Que toute personne se prévalant du présent Code s'oblige à en respecter l'intégralité des articles dans sa version en vigueur. Il sera publié régulièrement dans sa version actualisée.

L'évolution de ce document est de la responsabilité de l'Assemblée Générale du Clusif, sur proposition de la Commission Permanente Régulation.

NB Le présent Préambule ne fait pas partie du Code d'Ethique.

II - RÈGLES GÉNÉRALES

Définition de l'intervenant

On entend par intervenant, toute personne physique, qu'elle agisse à titre indépendant ou pour le compte d'une personne morale avec laquelle elle est liée par contrat, dès lors qu'elle exécute un acte professionnel de nature prestation intellectuelle en sécurité des systèmes d'information.

Principes Généraux

Article 1 - Déontologie générale

L'intervenant ne doit pas revendiquer une compétence ou une expérience qu'il ne possède pas.

S'il se réfère à des méthodes, procédures, techniques normalisées ou connues, il doit l'indiquer. A contrario, s'il ne les utilise pas formellement et complètement, il doit le signaler expressément. Il doit expliciter les raisons de ses choix et recommandations.

Article 2 - Compétence et expérience

L'intervenant doit pouvoir faire état de son curriculum-vitae exact et complet, ainsi que ses références personnelles (sans enfreindre les règles de confidentialité).

Article 3 - Obligation de compétence

L'intervenant doit pouvoir justifier d'une compétence et d'une expérience dans le domaine d'intervention pour lequel il est appelé.

L'intervenant doit se tenir en permanence informé de toutes les obligations (déontologiques, réglementaires, juridiques, etc.) qui lui incombent et qui incombent à ses clients, ainsi que toutes les normes (nationales et internationales selon le cas) qui s'appliquent dans son domaine.

L'intervenant doit se tenir en permanence informé des travaux des structures nationales ou internationales jouant un rôle en matière de sécurité.

L'intervenant doit connaître et pouvoir expliciter les caractéristiques des principales méthodes ou produits spécifiques dans les domaines de compétence dont se prévaut ledit intervenant.

Article 4 - Neutralité

L'intervenant doit respecter une stricte objectivité dans les conseils ou les recommandations qu'il formulera dans le seul intérêt de son client. Cette clause s'applique notamment dans le cas de plusieurs missions susceptibles d'être menées chez le même client ou des clients différents.

Devoirs envers les clients

Article 5 - Indépendance

L'intervenant doit indiquer clairement l'ensemble des domaines couverts par son activité, ainsi que l'ensemble des produits et services qu'il propose. Il doit indiquer les liens d'intérêts notamment salariaux ou financiers qu'il possède avec des tiers qui pourraient être concernés par l'exécution ou les conséquences de la mission.

Article 6 - Confidentialité

L'intervenant s'engage à respecter une stricte confidentialité des informations qui lui sont confiées, ou qu'il peut voir, entendre ou comprendre dans le cadre de ses missions ou toute activités professionnelles. Il s'engage à protéger le secret des documents qu'il détient dans le cadre de ses missions ou qui lui sont confiées.

L'intervenant s'engage à ne déroger à la rèle générale de confidentialité des informations de ces clients qu'après accord écrit exprès du client. Cette règle s'applique aux références des clients, aux missions effectuées et aux éléments du curriculum-vitae.

L'intervenant s'engage à faire respecter cette obligations de confidentialité par ses collaborateurs et, de manière générale, toute personne intervenant sous sa responsabilité dans le cadre d'une mission.

Article 7 - Information du client

L'intervenant s'oblige, pendant la durée de sa mission à informer son client sur les évolutions (méthodes, techniques, procédures, obligations) qui surviennent dans le champ de son intervention. Au-delà de la période d'exécution de la mission, l'intervenant a en outre obligation d'informer son client lors de la découverte de failles en rapport avec la mission initiale, dans le cas d'un défaut caché lié à une erreur de l'intervenant.

Article 8 - Support du client

Si l'intervenant n'est plus en mesure d'aider son client, il doit l'orienter vers des professionnels dont il connaît la compétence.

Article 9 - Assurance de la responsabilité professionnelle

L'intervenant ou le cas échéant ses commettants ou la personne morale à laquelle il est contractuellement lié, s'engage à souscrire une assurance couvrant se Resposabilité Civile contractuelle ou extra-contractuelle fondée sur les recours de droit privé ou de droit public dans le cadre de son activité professionnelle. Cette garantie doit être maintenue en vigueur :

- pendant toute la durée de l'intervention ou de la prestation ;

- et postérieurement à celle-ci, durant une période subséquente d'une durée adéquate.

L'intervenant s'oblige à la demande à produire une attestation de l'assurance précisant les garanties et les capitaux souscrits.

Devoirs envers les confrères

Article 10 - Confidentialité

L'intervenant s'engage à respecter une stricte confidentialité des informations qui lui sont confiées, ou qu'il peut voir, entendre ou comprendre dans le cadre de ses missions ou de toute activité professionnelle, que ces informations concernent ses clients ou ses confrères. Il s'engage à protéger le secret des document qu'il détient ou qui lui sont confiés;

L'intervenant s'engage à ne déroger à la règle générale de confidentialité des informations que dans le cas de litige entre deux confrères porté devant l'arbitrage de ses pairs réunis dans une commission ad hoc (elle-même soumise aux règles de confidentialité), sous réserve de l'accord exprès des tiers impliqués par la divulgation.

Article 11 - Respect des confrères

L'intervenant s'interdit de dénigrer ses confrères et notamment auprès de clients ou à l'occasion de réunions professionnelles, de conférences ou auprès de la presse.

Il s'oblige à respecter les principes de loyauté et de libre concurrence.

Devoirs envers les tiers

article 12 - Confidentialité

L'intervenant s'engage à ne déroger à la règle générale de confidentialité des informations que dans les cas prévus par la loi.

III - PARTIE APPLICABLE AUX CONSULTANTS AU NIVEAU SDSSI*

Article 1 - Cohérence de l'étude

Lors d'un projet de type SDSSI, conformément à son obligation d'information, le consultant doit attirer l'attention de son client sur le caractère éventuellement incomplet ou incohérent d'une étude et lui conseiller une démarche corrective.

Article 2 - Engagement de l'entreprise

Le consultant doit faire en sorte d'obtenir la collaboration effective des responsables et des acteurs de l'entreprise et en particulier de la direction générale. Il doit signaler toute difficulté dans la réalisation de sa mission.

Article 3 - Engagement du consultant

L'engagement du consultant doit être défini à chaque étape de son étude, notamment en ce qui concerne le mode opératoire et la nature des résultats fournis.

Article 4 - Qualité du consultant

Le consultant responsable doit pouvoir justifier d'une expérience professionnelle reconnue. Il doit par ailleurs s'impliquer de manière effective dans les différentes étapes du projet.

Article 5 - Obligation de qualité

Le consultant doit notamment s'efforcer de vérifier la pertinence et l'authenticité des informations qui lui sont fournies. Il doit expliciter ses propres conclusions.

Article 6 - Utilisation des moyens

Le consultant doit employer au mieux les moyens mis à sa disposition par le client et dans l'équipe d'intervention. Il doit signaler dès qu'il en a connaissance tout risque d'insuffisance quantitative ou qualitative de ces moyens.

* SDSSI : Schéma Directeur Sécurité des Systèmes d'Information.

IV - PARTIE APPLICABLE AUX INTERVENANTS AU NIVEAU CONCEPTION DÉTAILLÉE

Article 1 - Etude préalable

L'intervenant doit attirer l'attention sur la nécessité d'intégrer toute étude détaillée dans un SDSSI. Il doit la déconseiller si elle ne repose pas au moins sur une analyse préalable du risque à couvrir.

Article 2 - Engagement de l'entreprise

L'intervenant doit faire en sorte d'obtenir la collaboration des responsables et acteurs de l'entreprise. Il doit avoir au sein de l'entreprise un ou plusieurs correspondants indentifiés. Il doit signaler toute difficulté dans la réalisation de sa mission.

Article 3 - Qualité de l'étude

L'intervenant doit proposer une solution adaptée aux besoins spécifiques de l'entreprise. Il s'oblige à fournir les éléments nécessaires à la compréhension par des tiers pour la phase de réalisation.

Article 4 - Utilisation des moyens

L'intervenant doit employer au mieux les moyens mis à sa disposition. Il doit signaler dès qu'il en a connaissance tout risque d'insuffisance de ces moyens.

V - PARTIE APPLICABLE AUX INTERVENANTS AU NIVEAU RÉALISATION

Article 1 - Cahier des charges

L'intervenant doit attirer l'attention sur la nécessité de disposer d'un cahier des charges précis et détaillé avant de procéder à la mise en place des moyens.

Article 2 - Engagement de l'entreprise

L'intervenant doit faire en sorte de disposer au sein de l'entreprise de correspondants identifiés, domaine par domaine, avec une disponibilité suffisante. Il doit signaler toute difficulté dans la réalisation de sa mission.

Article 3 - Qualité de l'équipe de réalisation

L'intervenant doit s'assurer de la compétence et de l'expérience des personnes employées à la réalisation pendant toute la durée du chantier.

Article 4 - Qualité de la solution

L'intervenant doit mettre en place une solution adaptée aux besoins spécifiques de l'entreprise. Il s'oblige à fournir les éléments nécessaires à la pérennité de la solution (en particulier la documentation).

Article 5 - Qualité de l'intervenant

L'intervenant doit s'efforcer de minimiser les perturbations liées à son intervention sur le fonctionnement de l'entreprise. Il doit attirer l'attention de son client sur les mesures complémentaires à mettre en oeuvre pour pallier les dysfonctionnements engendrés pendant la période de mise en place.

Article 6 - Utilisation des moyens

L'intervenant doit employer au mieux les moyens mis à sa disposition par le client et dans l'équipe d'intervention.

Il doit signaler dès qu'il en a connaissance tout risque d'insuffisance quantitative ou qualitative de ces moyens.

V - PARTIE APPLICABLE AUX INTERVENANTS AU NIVEAU CONTRÔLE

Article 1 - Nature de la prestation

Le contrôle s'applique à toute intervention comprenant tout ou partie du SDSSI, de la conception détaillée, de la réalisation, de la maintenance et à l'application effective des résultats de cette intervention.

Le rôle du l'intervenant est d'attirer l'attention sur les faiblesses ou lacunes par rapport au contexte du client qui doit être désigné et daté dans la définition de la mission. Le contrôle n'est pas une appréciation personnelle portée sur le système de sécurité.

Article 2 - Indépendance de l'intervenant

S'ils existent, les éventuels liens d'intérêts de l'intervenant pressenti avec les concepteurs ou les réalisateurs lui interdisent de réaliser une intervention de contrôle.

Article 3 - Engagement de l'entreprise

L'intervenant doit faire en sorte de disposer de toute les autorisations et de tous les accès (aux personnes, documents, matériels, logiciels, etc.). Il doit signaler toute difficulté dans la réalisation de sa mission. Il doit pouvoir en particulier intervenir de manière impromptue s'il le souhaite.

Article 4 - Engagement de l'intervenant

L'intervenant doit s'efforcer de minimiser les perturbation liées à son intervention sur le fonctionnement de l'entreprise.

V - PARTIE APPLICABLE AUX INTERVENANTS AU NIVEAU MAINTENANCE

Article 1 - Nature de la prestation

La maintenance est une opération visant à préserver ou à rétablir la disponibilité initiale du système. Elle doit faire l'objet d'une offre commerciale et d'un contrat spécifique indépendants de la réalisation.

Article 3 - Qualité de la prestation

L'intervenant doit s'efforcer de réparer dans le meilleur délai. Il doit proposer au client une solution de substitution si elle est de nature à rétablir plus rapidement une disponibilité au moins partielle du système. S'il décèle un défaut structurel, une cause possible de dysfonctionnement ou une inadéquation au contexte du client, il doit le signaler à ce dernier.

Article 4 - Devoirs envers les confrères

L'intervenant doit, le cas échéant, conseiller à son client de faire intervenir les autres prestataires de maintenance susceptibles d'être impliqués dans la réparation. Il doit s'efforcer de collaborer avec eux afin de déterminer les causes exactes de la défaillance.

Article 5 - Engagement de l'Intervenant

L'intervenant doit s'efforcer de minimiser les perturbations liées à son intervention sur le fonctionnement de l'entreprise.