ANCS

الوكالة الوطنية للسلامة السيبرنية

Agence Nationale de la Cyber Sécurité

CODE D'ETHIQUE PROFESSIONNELLE POUR LES EXPERTS AUDITEURS HABILITES PAR L'ANCS A EXERCER L'ACTIVITE D'AUDIT DANS LE DOMAINE DE LA CYBERSECURITE -PERSONNES MORALES-

Préambule

L'expert auditeur Personne Morale habilité par l'ANCS à exercer l'activité d'audit dans le domaine de la cybersécurité (désigné ci-après par "le bureau d'audit"), s'engage à respecter les principes et les règles définis dans le présent code d'éthique professionnelle.
Le non-respect de ce code peut entraîner à son encontre des mesures disciplinaires qui peuvent aller jusqu'à l'arrêt définitif de l'exercice de l'activité d'audit.

SECTION 1 : Déontologie générale

- Le bureau d'audit doit réaliser l'audit de manière loyale avec objectivité, diligence nécessaire et professionnalisme, conformément aux normes et aux meilleures pratiques professionnelles, dans le respect de l'audité, de son personnel et de ses infrastructures.
- Les informations sensibles relatives aux audits, et notamment les preuves, les constats et les rapports d'audit, doivent être protégés au minimum au niveau Diffusion Restreinte. Leur traitement doit être conforme aux normes et standards en matière de classification, de sauvegarde et d'archivage des données.
- Le bureau d'audit doit veiller à ce que les informations qu'il fournit, y compris à des fins publicitaires, ne soient ni fausses ni trompeuses.
- Le bureau d'audit doit encourager à assimiler, accepter et améliorer les solutions et mesures de sécurité, et décourager les pratiques non sécurisées.
- Le bureau d'audit doit veiller à contribuer à la conformité aux normes, aux procédures et aux mesures de réglementation appropriées aux systèmes d'information.
- Le bureau d'audit est tenu de respecter la législation et la réglementation en vigueur, notamment en matière de traitements de données à caractère personnel, de propriété intellectuelle et de lutte contre la fraude informatique.
- Le bureau d'audit doit s'acquitter de ses devoirs avec probité envers l'audité, l'ANCS, et ses confrères.
- Un processus disciplinaire doit être mis en place par le bureau d'audit à l'intention des salariés ayant enfreint les règles de sécurité ou la charte d'éthique.

SECTION 2 : Conduite de l'expert auditeur

Article 1 : Confidentialité

- Le bureau d'audit doit préserver la confidentialité des informations obtenues dans le cadre de ses missions, à moins qu'une communication ne soit requise par une autorité judiciaire ou une divulgation exigée par l'ANCS. Ces informations ne doivent ni être utilisées pour en tirer un bénéfice personnel ni communiquées à des tiers non autorisés.

Article 2 : Impartialité

- Le bureau d'audit doit réaliser l'audit de manière indépendante et impartiale, conformément aux normes professionnelles.
- Le bureau d'audit doit veiller à ne pas se retrouver dans des situations qui risquent d'affecter son jugement objectif ou de limiter son indépendance. Il doit éviter de se laisser influencer ou mettre sous pression.

- Le bureau d'audit ne doit pas réaliser l'audit de sécurité d'un système d'information auquel il a participé, que ce soit à l'élaboration, à la mise en œuvre ou à l'entretien de l'un de ses composants, au cours des deux années précédant la mission d'audit.

Article 3 : Professionnalisme

- Le bureau d'audit doit accepter d'entreprendre uniquement des missions d'audit pour lesquelles il maîtrise l'environnement et les technologies associées, et qu'il juge pouvoir accomplir dans leur totalité de manière professionnelle et dans les délais impartis.
- Le bureau d'audit doit veiller à présenter les CV de ses experts dont le contenu est exact et mis à jour à chaque fois que l'occasion se présente.
- Le bureau d'audit doit prendre en considération les dispositions appropriées pour couvrir les risques liés à ses prestations d'audit.
- Le bureau d'audit assume la responsabilité de l'audit qu'il réalise pour le compte de l'audité, notamment en cas de dommages éventuels causés au cours de l'audit.

Article 4 : Relation avec l'audité

- Le bureau d'audit doit faire preuve de respect personnel et professionnel à l'égard de l'audité et agir avec tact.
- Le bureau d'audit doit veiller à ne pas dépasser la limite de la confiance et des privilèges qui lui sont attribués dans le cadre de l'audit.

Article 5 : Relation avec l'ANCS

- Le bureau d'audit ne doit participer à une mission d'audit en tant qu'expert auditeur habilité par l'ANCS que lorsque sa situation est conforme aux exigences du cahier des charges d'exercice de l'activité d'audit.
- Le bureau d'audit doit communiquer à l'ANCS un rapport électronique d'activités annuel, accompagné d'une déclaration trimestrielle des salaires et des salariés auprès de la CNSS.
- Le bureau d'audit doit transmettre à l'ANCS les informations et les documents demandés dans les délais.
- Le bureau d'audit doit notifier l'ANCS par voie électronique de tout changement survenue par rapport aux conditions initiales d'exercice de l'activité d'audit, au plus tard dans un délai d'un mois à compter de la date de ce changement.
- Le bureau d'audit est tenu, lors de la réalisation de l'audit, d'informer immédiatement l'ANCS lorsqu'il découvre des risques de sécurité graves pouvant affecter la sécurité du cyberespace et il est tenu également d'alerter l'organisme concerné pour prendre les contremesures nécessaires.

Article 6 : Relation avec les confrères

- Le bureau d'audit doit respecter ses confrères et éviter de toucher à leur réputation par malveillance ou négligence.

Article 7 : Mise à niveau et amélioration des compétences

- Le bureau d'audit doit veiller constamment à la formation continue de ses experts pour la mise à niveau et l'amélioration de leurs compétences professionnelles d'ordre réglementaire, normatif et technologique en relation avec le domaine de la cybersécurité.
- Le bureau d'audit doit veiller à ce que chaque expert déclaré auprès de l'ANCS assure une session de formation dans le domaine de la cybersécurité pendant au moins trois jours ou suit une formation dans le domaine, au moins une fois tous les trois ans.
- Le bureau d'audit doit encadrer au moins un stagiaire pendant une période minimale de trois mois pour l'exercice de l'activité d'audit en matière de cybersécurité.

Article 8 : Moyens techniques et matériels

- Le bureau d'audit doit détenir d'un manuel de procédures organisationnelles et techniques permettant d'assurer la qualité de l'audit et de protéger les informations et données récupérées et traitées.
- Le bureau d'audit doit utiliser des versions récentes des outils d'audit tout en assurant une complétude correcte des différentes phases d'audit, en particulier la phase d'audit technique. Pour tout produit commercial, il doit l'utiliser avec une licence valide permettant son usage correct pour de telles missions. Pour tout outil disponible dans le domaine du logiciel libre ou gratuit, il doit faire référence à une source officielle ou une communauté active.
- Le bureau d'audit doit obtenir un accord formel préalable de l'audité avant toute utilisation d'un outil d'audit basé sur le cloud.

SECTION 3 : Conduite de la mission d'audit

Article 9 : Respect du règlement intérieur de l'audité

- Le bureau d'audit doit respecter les consignes applicables au règlement intérieur de l'audité et examiner tous les contrats et les accords, explicites ou implicites.

Article 10 : Ressources requises pour l'audit

- Le bureau d'audit doit demander toutes les ressources requises pour la mission (documents, habilitations, logistiques, etc), en particulier le rapport d'audit précédent.
- Le bureau d'audit doit mentionner, au niveau du rapport d'audit, toute ressource demandée de l'audité et non fournie, et dont son absence a impacté la qualité des résultats de l'audit.

Article 11 : Equipe intervenante

- Pour toute mission conduite sous sa supervision, le bureau d'audit doit veiller à présenter à l'audité, lors de la réunion d'ouverture, l'équipe intervenante ainsi que l'affectation de chacun. Toute modification de la composition de cette équipe doit être approuvée par l'audité.

Article 12 : Périmètre de l'audit

- Le bureau d'audit doit respecter le périmètre de l'audit annoncé par l'audité. Tout changement au niveau du périmètre de l'audit doit être approuvé par l'audité.
- Le bureau d'audit doit veiller à examiner chaque composant du périmètre selon la méthodologie d'audit approuvée par l'audité.
- Le bureau d'audit ne doit procéder à l'échantillonnage que suite à l'approbation par l'audité de la méthode d'échantillonnage.

Article 13 : Plan d'audit

- Le bureau d'audit doit préparer un plan d'audit détaillant la nature, les objectifs, le calendrier, l'étendue et les ressources nécessaires pour l'audit, en particulier pour les tests intrusifs, conformément à ce qui a été convenu lors de la réunion d'ouverture.
- Le bureau d'audit doit veiller à respecter ce plan, en particulier les interventions sur terrain.
- Le bureau d'audit doit veiller à appuyer chaque intervention sur terrain par un PV signé par les personnes impliquées.

Article 14 : Normes, méthodologies et outils d'audit utilisés

- Le bureau d'audit doit réaliser l'audit conformément au référentiel défini par l'ANCS.

- Le bureau d'audit doit adopter une méthodologie d'audit (organisationnel, physique, technique, analyse de risque) adaptée à l'audité et devant être respectée et mentionnée au niveau du rapport.
- Le bureau d'audit doit veiller à utiliser les outils de test les plus adaptés pour chaque système cible.

Article 15 : Constats de l'audit

- Le bureau d'audit doit présenter des constats fiables, pertinents, formulés clairement, de manière synthétique et sans équivoque et qui doivent être perçus comme tels par toute tierce personne bien informée.
- Le bureau d'audit doit éviter de limiter ses constats uniquement aux résultats de la revue documentaire ou aux résultats bruts des rapports générés par les outils de test automatisé de vulnérabilités. En l'absence de l'interviewé ou de réponse claire, éviter de répondre par soi-même au questionnaire et veiller, tout au long de l'audit, à conserver une attitude impartiale caractérisée par l'absence de tout préjugé.
- Le bureau d'audit doit veiller à examiner minutieusement les configurations des différents composants, en plus des tests automatisés, et les confronter avec la politique de sécurité de chacun, même si cette dernière est informelle.
- Le bureau d'audit doit éviter de se baser uniquement sur les résultats des tests intrusifs pour accomplir l'audit technique.
- Le bureau d'audit doit éviter de donner des constats sans présenter les éléments probants suffisants, fiables, pertinents et utiles.
- Le bureau d'audit doit éviter de généraliser ses constats suite à des vérifications sur un échantillon non significatif.
- Le bureau d'audit ne doit pas se limiter à mentionner l'existence d'une politique ou procédure, mais il doit étudier son efficacité.

Article 16 : Plan d'action

- Le bureau d'audit doit proposer un plan d'action personnalisé, réaliste et optimisé, qui s'adapte avec la réalité humaine, financière et culturelle de l'audité et qui supporte les projets futurs, à court et à moyen terme, de l'audité.
- Le bureau d'audit doit veiller à étudier les solutions proposées avec l'audité en termes de faisabilité et efficacité.
- Le bureau d'audit doit éviter de proposer des solutions orientées vers des produits commerciaux.
- Le bureau d'audit doit éviter toute situation de conflit d'intérêts entre son rôle d'auditeur et celui de maître d'œuvre.
- Le bureau d'audit doit éviter de proposer toujours les mêmes solutions à différents audités sans prendre en compte les besoins spécifiques de chacun.

Article 17 : Livrables de l'audit

- Le bureau d'audit doit se conformer rigoureusement au modèle de rapport d'audit fourni par l'ANCS.
- Le bureau d'audit doit être responsable du contenu des rapports d'audit délivrés à l'audité, et il doit montrer son engagement par la signature du rapport.
- Le bureau d'audit ne doit ni distribuer, ni diffuser, ni communiquer les livrables, quelque soit leur forme (papier, magnétique, électronique ou autre), sans le consentement écrit de l'audité. Tous les livrables sont la propriété exclusive de l'audité.

Article 18 : Transparence avec l'audité

- Le bureau d'audit doit agir en toute transparence avec l'audité et l'informer de toute action sur son système d'information à temps, en particulier de toute brèche de sécurité observée même si le système cible n'est pas couvert par le périmètre de l'audit.
- Le bureau d'audit doit informer l'audité de toute manipulation qui agit sur son système d'information même de manière passive ou indirecte.

Article 19 : Avis de l'ANCS sur le rapport d'audit

- Le bureau d'audit doit assurer le traitement des remarques soulevées par l'ANCS suite à l'étude du rapport d'audit relatif à une mission conduite sous sa supervision.
- Le bureau d'audit doit entreprendre les actions nécessaires pour combler les manquements identifiés dans l'avis de l'ANCS.

Je soussigné ....., le représentant juridique du bureau d'audit ....., titulaire de l'identifiant fiscal ....., m'engage à respecter les dispositions du présent Code d'éthique professionnelle, et j'assume mes responsabilités face à toute infraction.

Cachet et signature du représentant juridique
(Sur toutes les pages)