

CODE DEONTOLOGIQUE DES PASSI

EXPOSE PREALABLE

Le présent code déontologique définit les principes déontologiques et règles de conduite applicables aux Prestataires d'Audit de Sécurité des Systèmes d'Information (PASSI) agréé par l'ANSSI.

Le PASSI s'engage à respecter les principes et les règles définis dans le présent code déontologique. Le non-respect du présent code peut entraîner à son encontre des sanctions qui peuvent aller jusqu'au retrait définitif de l'agrément.

PRINCIPES FONDAMENTAUX

- a. Le PASSI doit réaliser l'audit de manière loyale, indépendante et impartiale, avec la diligence nécessaire, conformément aux normes professionnelles et dans le respect de l'audité, de son personnel et de ses infrastructures.
- b. Le PASSI doit garantir la confidentialité des informations liées aux missions d'audit, à moins qu'une communication ne soit requise par une autorité judiciaire ou une divulgation exigée par l'ANSSI. Ces informations ne doivent pas être utilisées pour en tirer un bénéfice personnel ni communiquées à des tiers non autorisés.
- c. Le PASSI assume la responsabilité de l'audit qu'il réalise pour le compte de l'audité, en particulier des dommages éventuellement causés au cours de l'audit.
- d. Les auditeurs du PASSI ne recourent qu'aux méthodes, outils et techniques validés par le prestataire.
- e. Les auditeurs du PASSI signalent au client tout contenu manifestement illicite découvert durant la prestation.
- f. Le PASSI doit prendre en considération les dispositions appropriées pour couvrir les risques résultant de ses prestations d'audit.
- g. 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. Le traitement de ces données doit être conforme aux normes et standards relatifs à leur classification, sauvegarde et archivage.

- h. Le PASSI doit garantir que les informations qu'il fournit, y compris la publicité, ne sont ni fausses ni trompeuses.
- i. Un processus disciplinaire doit être élaboré par le prestataire d'audit à l'intention des salariés ayant enfreint les règles de sécurité ou la charte d'éthique.
- j. Le PASSI doit informer l'ANSSI, sans délai excessif, de tout incident de sécurité ayant pu impacter la confidentialité, l'intégrité ou la disponibilité des informations traitées ou des outils utilisés dans le cadre de ses missions.
- k. Le PASSI doit notifier à l'ANSSI toute modification substantielle de son organisation pouvant impacter le maintien de son agrément (changement de gouvernance, réorganisation interne, perte de personnel clé, etc.).
- l. Le PASSI peut sous-traiter une partie de l'audit, après l'accord écrit et préalable de l'audité, à un prestataire d'audit agréé et signataire du présent code .
- m. Le PASSI doit veiller au respect de ses confrères et éviter de toucher à leur réputation par malveillance ou indifférence.

Je soussigné, représentant légal de la société, dont le registre de commerce est, m'engage à respecter les dispositions du présent code déontologique.

Lu et Approuvé, le / /

Signature et Cachet