RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

Label ExpertCyber

Recueil des critères d'évaluation des candidatures

Version 3.1 – Novembre 2025

Table des matières

I. Principes de base

1. Élaboration des critères d'évaluation

Le présent recueil de critères du « Label ExpertCyber » représente un instrument de valorisation de l'expertise en sécurité numérique de prestataires de service exerçant des activités d'installation, de maintenance et d'assistance informatique auprès de leurs clients.

Il s'appuie sur les principes généraux suivants :

- une approche globale de l'évaluation des prestataires ayant démontré un niveau de maturité minimum, de la formation du personnel à l'élaboration de procédures internes en passant par la qualité des services délivrés aux clients ;
- une sélection de critères incontournables pour la profession et ses parties prenantes (internes et externes) qui sont d'application obligatoire ;
- une sélection de critères importants pour la profession et ses parties prenantes (internes et externes) dont l'application peut varier et qui nécessitent une appréciation d'un auditeur. Ces critères abordent des compétences complémentaires aux compétences obligatoires et sont vus comme une valorisation des prestataires les plus avancés et une incitation à monter en compétence pour l'ensemble de la profession ;
- les critères d'évaluation dans leur globalité sont accessibles mais engageants ;
- le référentiel promeut une approche progressive et incitative à l'amélioration continue ;
- un barème de points est associé à chaque critère. Le prestataire candidat au label doit démontrer qu'il atteint le seuil de points minimum d'obtention du label et qu'il satisfait dans le même temps à tous les critères obligatoires.

2. Périmètre des compétences évaluées par le « Label ExpertCyber »

Le « Label ExpertCyber » vise à reconnaître la qualité des compétences de prestataires techniques dans tout ou partie des champs d'expertise suivants :

- Les principales attaques et activités malveillantes rencontrées par ses clients, leurs caractéristiques et impacts principaux ;
    - les principes de propagation d'une attaque sur un système d'information, par le réseau ou par support amovible ;
    - les principes de l'escalade de privilèges ;
    - l'exfiltration de données ;
- La sécurisation des architectures et technologies des systèmes d'informations ;
    - leurs vulnérabilités et leurs mécanismes d'administration ;
    - le fonctionnement, la sécurisation et les vulnérabilités des principaux systèmes d'exploitation (Microsoft, UNIX, GNU/Linux, MacOS) et solutions de virtualisation ;
    - les protocoles et architectures réseau, leurs vulnérabilités et leur sécurisation.
- Les applications et leurs vulnérabilités : applications bureautiques, navigateurs Internet, serveurs Web, bases de données, serveurs de messagerie, progiciels, etc.
- Les outils d'analyse : analyse de systèmes (antivirus, mémoire, disques), analyse de journaux (signature, système, applicatif ou réseau) ;
- La connaissance des autorités impliquées dans le traitement d'un incident informatique ;
- La connaissance des principales qualifications juridiques des faits de cybermalveillance qu'ils sont amenés à traiter, ainsi que les juridictions

compétentes à en connaître, au plan pénal et civil, mais également sur le plan territorial.

Le prestataire candidat doit avoir les qualités suivantes lors d'une intervention :

- Savoir définir et gérer les priorités, en particulier en situation de crise ;
- Savoir synthétiser et restituer l'information utile aux clients pour du personnel technique et non technique ;
- Savoir sensibiliser à la résilience aux sinistres (PCA, PRA,…).

3. Critères d'éligibilité administrative relatifs aux entreprises candidates

Le siège statutaire, administration centrale et principal établissement du prestataire doivent être établis au sein d'un État membre de l'Union Européenne.

L'établissement candidat à la labellisation doit être situé sur le territoire français et justifier d'une existence juridique effective d'au moins un an à la date de soumission de la candidature.

II. Critères d'évaluation du prestataire

1. Critère relatif aux documents et informations transmis lors de l'évaluation

a. Authenticité des documents et informations transmis [obligatoire]

Exigence :
Dans le cadre de la procédure d'évaluation du label, le prestataire doit s'engager sur l'authenticité des documents et informations transmis.

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- Renseignement et signature de la trame de déclaration sur l'honneur

2. Critères relatifs au respect du champ d'application du référentiel

a. Activités et prestations [obligatoire]

Exigence :
Le prestataire doit obligatoirement réaliser à la fois des prestations d'installation, de maintenance et d'assistance informatique dans le domaine de la cybersécurité (dépannage, réponse à incident de sécurité) lors desquelles il met en œuvre un large éventail de compétences en sécurité informatique.

Il peut réaliser d'autres prestations qui ne sont pas inclues dans le champ d'application du label. Celles-ci ne seront bien entendu pas auditées dans le cadre de la labellisation.

Les prestations externalisées par le prestataire à des sous-traitants ne sont pas concernées par le label. Les solutions (logiciels et matériels) déployées par le prestataire ne doivent pas être restreintes aux seuls produits développés par celui-ci.

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- Lien vers un site web du prestataire ou vers une page d'un réseau social détaillant les activités réalisées par le prestataire

- Brochure commerciale ou autre élément permettant de déterminer la nature des activités du prestataire

b. Domaines d'interventions techniques [obligatoire]

Exigence :

Le prestataire doit réaliser des prestations et interventions dans un ou plusieurs domaines techniques généralistes suivants :

- Infrastructure IT (PC, système d'exploitation, logiciels y compris SaaS, serveurs, …)
- Téléphonie (fixe et mobile).
- Web (sites internet, navigateurs web, …)

Les domaines d'intervention spécialisés comme par exemple l'informatique industrielle ne sont pas inclus dans le champ d'application du label.

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- Lien vers un site web du prestataire ou vers une page d'un réseau social détaillant les activités réalisées par le prestataire
- Brochure commerciale ou autre élément permettant de déterminer les domaines d'intervention du prestataire

c. Zones géographiques d'intervention sur site [obligatoire]

Exigence :

Le prestataire doit être en capacité d'intervenir physiquement sur les sites des clients basés en France dans son périmètre d'intervention. Le prestataire ne doit pas réaliser uniquement des télé-interventions ou des interventions sur des SI hébergés dans ses propres locaux.
Dans le cas d'un prestataire proposant uniquement la sécurisation de services en

nuage (cloud), celui-ci doit être en capacité d'intervenir physiquement sur les sites des clients basés en France, a minima en cas d'incident.

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- Déclaration d'une zone d'intervention sur site par le prestataire. Elle doit être cohérente avec les délais d'intervention sur lesquels le prestataire s'engage (GTI,…).

3. Critères relatifs à l'organisation interne du prestataire

a. Existence juridique [obligatoire]

Exigence :

Le prestataire doit être inscrit au registre du commerce et des sociétés pour le site concerné par la demande de labellisation (les prestataires disposant de plusieurs sites de production doivent candidater et présenter un dossier complet pour chaque site pour lequel ils souhaitent obtenir la labellisation).

Le prestataire doit respecter les critères d'éligibilité administratives mentionnés en section 3, page 6

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- Extrait K-bis ou Extrait K à jour datant de moins de 3 mois.
- Cas particulier : Les Opérateurs Publics de Services Numériques (OPSN) non-inscrits au RCS doivent fournir un avis de situation de l'INSEE mentionnant le numéro de SIRET du site objet de la labellisation.

b. Conformité de la situation de l'entreprise aux lois et réglementations relatives à son activité [obligatoire]

Exigence :

Le prestataire doit attester sur l'honneur du respect des lois et des réglementations en vigueur qui s'appliquent à son activité.

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- Renseignement et signature de la lettre d'attestation sur l'honneur présente en annexe de ce référentiel (voir Annexe 2) par le dirigeant de l'entité morale qui candidate au label.

c. Souscription d'une assurance [non-obligatoire]

Exigence :

Le prestataire doit souscrire à une assurance de responsabilité civile professionnelle ou RC Pro qui couvre le champ d'activité du label. L'attestation d'assurance doit mentionner clairement que les interventions sur les SI des clients du prestataire sont couvertes.

Le prestataire peut également souscrire à une assurance spécifique cyber couvrant son propre système d'information.

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- Attestation(s) RC Pro mentionnant de préférence clairement le champ d'activité du label ou mentionnant a minima les interventions sur les SI des clients.
- Le cas échéant, attestation d'assurance spécifique cyber, qui pourra apporter au candidat des points supplémentaires lors de l'examen de sa candidature.

d. Procédures liées à la sécurité de l'information [non-obligatoire]

Exigence :

Le prestataire doit prendre en compte la sécurité de l'information dans ses procédures à appliquer lors des interventions sur site client. Il doit également prendre en compte la sécurité de l'information dans ses procédures internes afin d'assurer la sécurité de son propre système d'information. Il peut s'inspirer des guides élaborés par l'ANSSI.

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- 2 procédure(s) à appliquer en cas d'interventions sur les SI des clients dans le cadre du champ d'activité du label (installation, maintenance, assistance).
- ET 1 procédure interne liée à la sécurité de l'information (par exemple une charte informatique ou une politique de sécurité).

e. Politique en matière de protection des données personnelles [obligatoire]

Exigence :

Le prestataire doit documenter sa stratégie en matière de respect du RGPD et protection des données personnelles en interne au sein de son organisme et dans ses relations avec ses clients.

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- Tout document montrant la prise en compte du RGPD et de ses enjeux par le prestataire dans ses processus internes (politique de protection des données personnelles, politique de confidentialité, désignation DPO…).
- ET Tout document montrant la prise en compte du RGPD et de ses enjeux par le prestataire à destination de ses clients (trame de contrat client intégrant des clauses contractuelles spécifiques, …).

f. Certifications ou labels en lien avec la gouvernance de la sécurité de l'information [non-obligatoire]

Exigence :

Le prestataire peut faire certifier ou labelliser son entreprise, son organisation ou ses employés pour répondre à des objectifs de gouvernance de la sécurité de l'information.

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- Certificat ou attestation de labellisation en cours de validité en lien avec la gouvernance de la sécurité de l'information et s'appliquant à l'organisation du prestataire (ISO 27001, ISO 27701, PASSI, etc.) ou à un de ses employés (Lead Implementer ISO 27001, Lead Cybersecurity Manager ISO 27032, EBIOS RM, …).

4. Critères relatifs aux compétences du prestataire

a. Gestion des compétences du personnel [non-obligatoire]

Exigence :

Le prestataire doit attester des compétences du personnel qui va être engagé sur les activités d'installation, de maintenance et d'assistance informatique en cas d'incident.

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- Curriculum Vitae à jour de plusieurs membres des équipes cyber rattachés au site à labelliser (maximum 5 CV) accompagnés obligatoirement d'un organigramme afin de situer les membres au sein des effectifs du prestataire (sauf dans le cas des auto-entrepreneurs). Ces CV doivent contenir des informations (adresse, …) permettant de les rattacher à l'unique site (implantation géographique) qui candidate au label.

b. Formation technique continue du personnel [non-obligatoire]

Exigence :

Le prestataire doit disposer de ressources compétentes et formées au moins sur les domaines suivants :

- Firewall, UTM (Unified Threat Management), administration/sécurisation de serveur (Microsoft, GNU/Linux, …) sur site et cloud.
- Sauvegarde
- Protection du poste de travail (antivirus, Endpoint Detection and Response, etc.)

Dans le cas d'un prestataire proposant uniquement la sécurisation de services en nuage (cloud), celui-ci doit également disposer de ressources compétentes et formées sur le domaine de la cybersécurité des systèmes en nuage (cloud).

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- Certificat(s) ou attestation(s) de formations ou de compétences en cours de validité ou délivré depuis moins de 2 ans (si pas de date de fin de validité) s'appliquant au personnel du prestataire en lien avec un ou plusieurs domaines de compétences listés concernant la maîtrise de solutions logicielles ou les principes de mise en œuvre. Les certificats de nature purement commerciale ne sont pas acceptés.
- Les descriptifs des contenus des formations réalisées

c. Adhésion à une organisation professionnelle [non-obligatoire]

Exigence :

Le prestataire peut adhérer à une organisation professionnelle (groupement d'entreprises ou syndicat professionnels en lien avec le numérique) ou avoir du personnel membre de clubs ou comités spécialisés (club ou comité de normalisation en lien avec la sécurité informatique) afin d'être informé des

évolutions de la profession, des bonnes pratiques et de bénéficier d'une aide dans les domaines juridique, social et réglementaire.

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- Une preuve d'adhésion en cours de validité à une organisation professionnelle en lien avec le numérique.
- Ou une preuve de participation à un club ou comité de normalisation en lien avec la sécurité informatique pour un des membres du personnel du prestataire.

d. Participation à cybermalveillance.gouv.fr [non-obligatoire]

Exigence :

Le prestataire peut être référencé sur la plateforme cybermalveillance.gouv.fr et ainsi bénéficier d'une sensibilisation aux bonnes pratiques et d'une veille régulière sur les problématiques de cybermalveillance.

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- Aucun élément à fournir. L'information de référencement ou non du prestataire sur la plateforme cybermalveillance.gouv.fr sera apportée à l'organisme d'évaluation par le GIP ACYMA.

e. Remontée d'incidents sur cybermalveillance.gouv.fr [non-obligatoire]

Exigence :

Le prestataire peut être un acteur de la lutte contre les actes de cybermalveillance en lien avec son référencement sur Cybermalveillance.gouv.fr en ayant effectué une ou plusieurs remontées d'incidents durant les deux dernières années.

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- Aucun élément à fournir. Le GIP ACYMA informera l'organisme d'évaluation sur le nombre de remontées d'incidents réalisées par le prestataire sur la plateforme Cybermalveillance.gouv.fr dans les deux dernières années.

f. Rapport d'intervention post-incident [non-obligatoire]

Exigence :

Au cours d'une intervention post-incident de sécurité, le prestataire doit analyser le ou les incidents de manière pertinente et proposer des solutions techniques appropriées à son client. Il doit également proposer des actions correctives pour que l'incident ne se reproduise plus. Tous ces éléments composent le rapport d'intervention post-incident de sécurité.

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- 1 rapport d'intervention (qui peut être réalisée sur site ou à distance), daté et pouvant être anonymisé par le candidat (sur justification), représentatif de l'activité du prestataire dans le domaine de l'assistance post-incident de sécurité informatique et datant de moins de 2 ans.

  S'il s'agit d'une intervention à distance elle doit être réalisée à partir d'un pays de l'Union Européenne par un salarié rattaché au site candidat à la labellisation et concerner des clients basés en France.

- ET la facture correspondante à l'intervention (ou le rapport annuel d'activité client faisant apparaître l'intervention, si la prise en charge de la prestation est incluse dans un accord cadre).

g. Rapport d'intervention de sécurisation [obligatoire]

Exigence :

Au cours d'une intervention de sécurisation d'un système d'information, en anticipation des incidents de sécurité, le prestataire doit analyser la ou les briques du SI à sécuriser en identifiant les vulnérabilités et mettre en application des solutions techniques et des mesures de sécurité appropriées en adéquation avec l'état de l'art du domaine de la cybersécurité (guides de l'ANSSI, normes, …). Tous ces éléments composent le rapport d'intervention de sécurisation.

L'intervention de sécurisation peut ne concerner qu'une seule brique du SI, comme par exemple les cas d'interventions suivants : sécurisation de l'Active Directory, installation et paramétrage de firewall, sécurisation des accès nomades et installation d'un VPN, la sécurisation des flux mails, découpage et configuration de VLAN, …

Les interventions se limitant à des installations ne nécessitant pas d'expertise technique (exemple : le déploiement d'antivirus) ne sont pas acceptables car elles ne permettent pas à l'auditeur d'apprécier l'expertise technique du prestataire.

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- 1 rapport d'intervention (qui peut être réalisée sur site ou à distance) anonymisé et daté représentatif de l'activité du prestataire dans le domaine de la sécurisation du SI et datant de moins de 2 ans. Ou les documents concernant la sécurisation du SI d'un client permettant d'apprécier l'intervention réalisée et le niveau de sécurité atteint.

  S'il s'agit d'une intervention à distance elle doit être réalisée à partir d'un pays de l'Union Européenne par un salarié rattaché au site candidat à la labellisation et concerner des clients basés en France.

- ET la facture détaillée ou l'ensemble des documents (financiers et contractuels), ou le rapport annuel d'activité client faisant apparaître l'intervention, si la prise en charge de la prestation est incluse dans un accord cadre.

Les rapports d'intervention doivent démontrer la compétence du prestataire et la qualité du paramétrage effectué. Ils doivent faire apparaître les éléments attestant du niveau et de la rigueur de l'intervention réalisée.

h. Réussite au Questionnaire technique [obligatoire]

Exigence :

Le prestataire doit disposer d'une base de connaissances suffisante en rapport avec les activités de prestation et de remédiation.

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- Résultat positif au Questionnaire technique.

  Le prestataire n'obtenant pas la moyenne des points au Questionnaire technique ne peut pas prétendre à l'obtention du label.

5. Critères relatifs aux services délivrés aux clients

a. Transparence du délai d'intervention [non-obligatoire]

Exigence :

Le prestataire doit être transparent auprès de ses clients sur ses délais d'intervention (garantie de temps d'intervention) et les en informer avant d'intervenir.

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- Clauses d'intervention appliquées par le prestataire
- Ou contrat-type utilisé par le prestataire pour une intervention

b. Transparence des tarifs appliqués [non-obligatoire]

Exigence :

Le prestataire doit être transparent auprès de ses clients sur les tarifs qu'il applique (tarifs précis ou fourchette de prix) et les en informer avant d'intervenir.

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- Brochure commerciale
- Ou lien vers son site web
- Devis type anonymisé
- Ou tout autre élément mentionnant les tarifs appliqués ou la fourchette de prix pratiqué pour des interventions

c. Devoir de conseil auprès des clients [non-obligatoire]

Exigence :

Le prestataire doit partager au moins une fois par trimestre des règles et conseils de sécurisation avec ses clients et prospects, notamment en synthétisant, vulgarisant et relayant les conseils donnés par les autorités compétentes et les pôles d'expertise.

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- Documents de sensibilisation que le prestataire fournit à ses clients
- Ou offres de conseil
- Ou extraits d'une newsletter du prestataire comportant des conseils en sécurité numérique pour ses clients
- Ou articles postés sur les réseaux sociaux

d. Conservation de preuves numériques [non-obligatoire]

Exigence :

Le prestataire doit savoir collecter et conserver une preuve numérique du ou des incidents afin de permettre à ses clients de déposer plainte.

Élément(s) de preuve(s) associé(s) à fournir par le prestataire :

- Description des méthodes de conservation de preuve associées à deux types d'incidents différents au choix (exemple de type d'incident : hameçonnage, rançongiciel, DDoS, arnaque au faux support technique, etc.).

  Contenu attendu d'une méthode de conservation de preuve :

  - Incident concerné par la méthode ;
  - Liste des preuves à conserver (documents, logs, mails, etc.) et justification de leur pertinence ;
  - Méthodologies de collecte et de conservation (copie, lieu et durée de conservation de la sauvegarde, …).

III. Barème et obtention du label

1. Barème de notations appliqué pour chaque critère d'évaluation

Famille de critères	N° Critère	Critère	Critère d'application obligatoire qui entraîne le rejet de la candidature en cas d'insatisfaction	Barème (Scoring)
Critère relatif aux documents et informations transmis lors de l'évaluation	1. a.	Authenticité des documents et informations transmis	x	0 point
Critères relatifs au respect du champ d'application du référentiel	2. a.	Activités et prestations	x	0 point
	2. b.	Domaines d'interventions techniques	x	0 point
	2. c.	Zones géographiques d'intervention sur site	x	0 point
Critères relatifs à l'organisation interne du prestataire	3. a.	Existence juridique	x	0 point
	3. b.	Conformité de la situation de l'entreprise aux lois et réglementations relatives à son activité	x	0 point
	3. c.	Souscription d'une assurance		4 points : - entre 0 et 2 points pour la RCPro selon l'appréciation de l'auditeur. - 2 points en cas d'assurance cyber couvrant le SI interne si la RCPro est complète.
	3. d.	Procédures liées à la sécurité de l'information		9 points : Entre 0 et 3 points par procédure selon l'appréciation de l'auditeur
	3. e.	Politique en matière de	x	5 points :

Famille de critères	N° Critère	Critère	Critère d'application obligatoire qui entraîne le rejet de la candidature en cas d'insatisfaction	Barème (Scoring)
		protection des données personnelles		- entre 0 et 4 points selon l'appréciation de l'auditeur - 1 point si le candidat à un DPO
	3. f.	Certifications ou labels en lien avec la gouvernance de la sécurité de l'information		2 points
Critères relatifs aux compétences du prestataire	4. a.	Gestion des compétences du personnel		Entre 0 et 2 points selon l'appréciation de l'auditeur
	4. b.	Formation technique continue du personnel		9 points : Entre 0 et 3 points attribués selon l'appréciation de l'auditeur pour chaque domaine de compétence couvert
	4. c.	Adhésion à une organisation professionnelle		3 points
	4. d.	Participation à Cybermalveillance.gouv.fr		4 points
	4. e.	Remontée d'incidents sur cybermalveillance.gouv.fr		4 points : 2 points par remontée d'incident réalisée durant les deux dernières années
	4. f.	Rapport d'intervention post-incident		Entre 0 et 15 points selon l'appréciation de l'auditeur.
	4. g.	Rapport d'intervention de	x	Entre 0 et 15

Famille de critères	N° Critère	Critère	Critère d'application obligatoire qui entraîne le rejet de la candidature en cas d'insatisfaction	Barème (Scoring)
		sécurisation		points selon l'appréciation de l'auditeur.
	4. h.	Réussite au QCM technique	x	10 points Pourcentage de bonnes réponses au QCM.
Critères relatifs aux services délivrés aux clients	5. a.	Transparence du délai d'intervention		3 points
	5. b.	Transparence des tarifs appliqués		2 points
	5. c.	Prestations de conseil auprès des clients		Entre 0 et 5 points selon l'appréciation de l'auditeur
	5. d.	Conservation de preuves numériques		Entre 0 et 8 points selon l'appréciation de l'auditeur

2. Obtention du label

Le prestataire obtient le label « ExpertCyber » lorsque:

- Il satisfait à tous les critères d'évaluation obligatoires
- Il obtient une note supérieure à la moyenne au Questionnaire technique (critère 4.h)
- Il obtient une note globale supérieure à 65/100 à la suite de l'évaluation.

ANNEXE 1 Lettre d'attestation sur l'honneur du respect législatif et réglementaire

Date :

Objet : Attestation sur l'honneur du respect législatif et règlementaire dans le cadre de la candidature au label ExpertCyber

Je soussigné……....

exerçant la fonction de ……

au sein de la société ……....

identifiée sous le n° SIREN : ……...

dont l'établissement qui candidate est situé au …….....

déclare sur l'honneur :

(i) que ma société, ou un membre de l'organe de gestion, d'administration, de direction ou de surveillance de ma société ou une personne physique qui détient un pouvoir de représentation, de décision ou de contrôle au sein de ma société n'ont pas fait l'objet au cours des 36 derniers mois qui précèdent la présente candidature au label :

de condamnation définitive pour l'une des infractions prévues aux articles 222-34 à 222-40,225-4-1,225-4-7,313-1,313-3,314-1,324-1,324-5,324-6,421-1 à 421-2-4,421-5,432-10,432-11,432-12 à 432-16,433-1,433-2,434-9,434-9-1,435-3,435-4,435-9,435-10,441-1 à 441-7,441-9,445-1 à 445-2-1 ou 450-1 du code pénal, aux articles 1741 à 1743,1746 ou 1747 du code général des impôts, ou pour recel de telles infractions ;

de sanction pour méconnaissance des obligations prévues aux articles L. 8221-1, L. 8221-3, L. 8221-5, L. 8231-1, L. 8241-1, L. 8251-1 et L. 8251-2 du code du travail ou de condamnation au titre de l'article L. 1146-1 du même code ou de l'article 225-1 du code pénal ;

(ii) que ma société a souscrit les déclarations lui incombant en matière fiscale ou sociale et a acquitté les impôts, taxes, contributions ou cotisations sociales exigibles à la date de dépôt de la candidature au label ;

(iii) que ma société n'est pas en état de liquidation judiciaire ou ne pas faire l'objet d'une procédure équivalente régie par un droit étranger ;

(iv) ne pas être déclaré en état de faillite personnelle ou ne pas faire l'objet d'une procédure équivalente régie par un droit étranger ;

(v) que ma société n'est pas admise au redressement judiciaire ou à une procédure équivalente régie par un droit étranger, sans justifier d'une habilitation à poursuivre son activité pendant la durée de validité du label;

(vi) que ma société n'a pas fait l'objet au cours des 36 derniers mois qui précèdent la présente candidature au label, de sanction ou de condamnation devenue définitive pour violation de la réglementation relative à la protection des données personnelles

Signature :

ANNEXE 2 Lettre d'attestation sur l'honneur d'authenticité des documents et informations transmis

Date :

Objet : Attestation sur l'honneur d'authenticité des documents et informations transmis

Je soussigné……....

exerçant la fonction de ……

au sein de la société ……....

identifiée sous le n° SIRET: ……....

dont l'établissement qui candidate est situé au …….....

déclare sur l'honneur :

que l'ensemble des documents et informations fournis dans le cadre de la procédure d'évaluation du label ExpertCyber sont authentiques

Signature :