

CONVENTION D'AUDIT DE CYBERSURVEILLANCE

CERT Santé

Statut : Validé | Classification : Publique | Version : 1.0

Agence du Numérique en Santé — CERT Santé
Édition : novembre 2026

La présente Convention d'Audit (« Convention ») est conclue :

ENTRE LES SOUSSIGNES :

L'Agence du Numérique en Santé, groupement d'intérêt public, dont le siège social est situé au 2-10 rue d'Oradour-sur-Glane, 75015 Paris,

Représentée par Jean-Baptiste LAPEYRIE

Agissant en qualité de Directeur Expertise, Innovation et International

Ci-après dénommé(e) l' « Auditeur »,

ET

Dénomination de la structure : .....

Forme juridique : .....

Dont le siège social est situé au :
.....

Représenté(e) par : .....

Agissant en qualité de : .....

Ci-après dénommé(e) l'« Audité ».

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

Sommaire

PREAMBULE 4

1. Objet 4
2. Autorisation de réalisation de l'audit 4
3. Nature et déroulement de l'audit 5
4. Rapport d'audit 5
5. Confidentialité 6
6. Protection des données à caractère personnel 6
   - 6.1. Finalités et responsabilités de traitement 7
   - 6.2. Catégories de données traitées 7
   - 6.3. Obligations de l'ANS en sa qualité de sous-traitant 8
   - 6.4. Obligation de l'Audité en sa qualité de responsable de traitement 9
   - 6.5. Sécurité et confidentialité des données personnelles 9
   - 6.6. Violation de données 9
   - 6.7. Droits des personnes concernées 10
   - 6.8. Durées de conservation 10
7. Communication entre les Parties 11
8. Engagement des Parties 11
9. Modalités financières 12
10. Responsabilités 12
11. Durée et date d'effet du protocole 12
12. Fin anticipée de la Convention 12
    - 12.1. Résiliation 12
    - 12.2. Manquement d'une Partie à ses engagements 13
13. Loi applicable et tribunaux compétents 13
14. Signature électronique 13

ANNEXE : DETAIL DE LA PRESTATION 14

La méthodologie, le périmètre, le détail des tests ainsi que les prérequis retenus par l'Auditeur et validés par l'Audité sont précisés de manière exhaustive dans la présente annexe. 14

I. Méthodologie 14
II. PLANNING ET CONTACT 16
III. Périmètre 16
IV. Prérequis 16
V. Précautions particulières 17

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

PREAMBULE

L'Agence du Numérique en Santé (ANS) est le groupement d'intérêt public prévu à l'article L.1111-24 du code de la santé publique chargé de favoriser le développement des systèmes d'information, des services et des outils numériques utilisés dans le cadre de la prise en charge sanitaire, ainsi que du suivi social et médico-social des usagers du système de santé. Elle vise également à permettre la coordination des actions des professionnels de santé, à promouvoir la télésanté, la recherche, le dépistage, la prévention, la veille et l'alerte sanitaires.

L'ANS a notamment pour mission de participer au renforcement de la sécurité des systèmes numériques en santé. Elle est responsable, seule ou aux côtés des autres autorités compétentes, de la gestion de dispositifs de sécurité opérationnelle destinés aux professionnels, notamment le dispositif national de cybersurveillance, l'appui aux structures et le traitement des incidents de sécurité des systèmes d'information.

Le CERT Santé est le service de réponse à incident de l'ANS chargé d'accompagner les établissements de santé, les organismes et services exerçant des activités de prévention, de diagnostic ou de soins, ainsi que les établissements et services médico-sociaux (ci-après « Bénéficiaires ») dans la gestion des incidents de sécurité des systèmes d'information. Il assure également une mission de prévention et d'alerte face aux menaces de cybersécurité, réalisant notamment des audits de l'exposition des systèmes d'information sur Internet.

Dans ce cadre, le CERT Santé réalise des audits de sécurité à destination et sur demande de ses Bénéficiaires. En conséquence, il est convenu ce qui suit.

1. Objet

L'Auditeur réalise sur demande de l'Audité un audit de sécurité dénommé la « Prestation », objet de la présente Convention.

La présente Convention a pour objet de :

- Définir la nature et le déroulement de la Prestation ;
- Définir les modalités selon lesquelles l'Auditeur réalisera la Prestation ;
- Formaliser l'acceptation par l'ensemble des Parties quant à l'exécution de la Prestation.

Il est entendu que la Prestation ne pourra pas débuter tant que le présent document n'aura pas été dûment complété et signé par les Parties.

2. Autorisation de réalisation de l'audit

L'Audité autorise l'Auditeur à réaliser l'audit sur les domaines qu'il a déclaré en annexe.

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

Cette autorisation couvre les tests réalisés sur les infrastructures sous maîtrise de l'Audité. Lorsque l'Audité externalise tout ou partie de son système d'information, il s'engage à informer et obtenir l'autorisation de son prestataire préalablement à la réalisation de l'audit.

3. Nature et déroulement de l'audit

La Prestation implique l'évaluation du niveau de sécurité et la détection de manière préventive des vulnérabilités présentes sur les domaines exposés sur Internet précisés par l'Audité en Annexe des présentes.

La Prestation se déroule en deux phases :

- Une première phase consistant en la collecte d'informations à partir de sources ouvertes sur Internet ;
- Une seconde phase consistant en la réalisation d'un audit de chacun des domaines du système d'information déclarés par l'Audité. Cette phase comprend :
    - Une cartographie des services et des ressources accessibles ;
    - Le test des comptes avec des identifiants faibles, des identifiants par défaut ou des identifiants qui ont fait l'objet d'une fuite sur Internet ;
    - L'utilisation des scanneurs généralistes / spécifiques afin de détecter d'éventuelles erreurs de configuration et / ou de défauts de mise à jour.

Contrairement à un test d'intrusion, il est à noter que lors de cet audit, les vulnérabilités pouvant présenter un risque pour la disponibilité du système ne sont pas testées (exemple : débordement de tampon, déni de service). Les vulnérabilités ne sont pas exploitées offensivement (pas de prise de contrôle à distance des serveurs).

Un rapport présentant les vulnérabilités identifiées, leur niveau de criticité et des mesures correctives est produit par l'ANS à l'issue de l'audit puis communiqué à l'Audité.

4. Rapport d'audit

A l'issue de la réalisation de l'audit, l'Auditeur délivre un rapport à l'Audité mis à disposition sur la plateforme Cybersurveillance.

Le rapport présente :

- Le périmètre de l'évaluation avec la liste des domaines et sous-domaines, accompagnée d'une cartographie des systèmes détectés ;
- Une synthèse managériale présentant le niveau de sécurité observé et de manière succincte la typologie des vulnérabilités identifiées ;
- Une synthèse technique présentant :
    - des vulnérabilités détectées et classées par niveau de criticité ;
    - un plan d'action de remédiation hiérarchisé ;
    - le détail des vulnérabilités identifiées, incluant pour chacune :

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

- la criticité ;
- le type de vulnérabilité (ou catégorie, telle qu'usurpation d'identité, défaut de configuration, etc.) ;
- le système d'information affecté ;
- la description de la vulnérabilité ;
- la recommandation associée pour sa correction.

5. Confidentialité

Relèvent de l'application du présent article toutes les informations qui sont transmises par toute Partie à l'autre Partie dans le cadre de l'exécution de la présente Convention, et qui sont désignées comme informations confidentielles lors de leur transmission. Seront également considérées comme informations confidentielles, les informations auxquelles chacune des Parties pourraient avoir accès dans le cadre de la Prestation.

Les Parties s'engagent à n'utiliser les informations confidentielles des autres Parties qu'en vue de la réalisation des objectifs prévus par la présente Convention.

Chacune des Parties s'engage à prendre toutes les mesures nécessaires en vue de la protection des informations confidentielles, et s'interdit d'en faire toute divulgation à des tiers, sauf accord préalable écrit de la Partie à laquelle appartiennent ces informations. La notion de tiers, désigne toute personne physique ou morale autre que l'Auditeur ; cela inclut des sous-traitants éventuels.

L'Auditeur s'engage à communiquer le rapport d'audit seulement à l'Audité et aux personnes impliquées dans l'activité de cybersurveillance au sein de l'ANS. Si une communication à un tiers s'avérait nécessaire, l'Auditeur ne pourrait alors diffuser le rapport d'audit qu'avec l'accord exprès de l'Audité.

Chaque Partie conserve la propriété pleine et entière des informations confidentielles qu'elle communique dans le cadre de la présente Convention.

La présente Convention ne saurait en aucune façon être interprétée comme conférant à l'une ou l'autre des Parties, qui reçoit les informations confidentielles, un droit quelconque sur (aux termes d'une licence ou par tout autre moyen) tout ou partie desdites informations.

Aucun droit de propriété industrielle et/ou intellectuelle n'est concédé à l'une ou l'autre des Parties sur la base des informations confidentielles reçues d'une autre Partie.

6. Protection des données à caractère personnel

La réalisation de la Prestation entraine un traitement de données à caractère personnel.

Les Parties concernées par la présente convention s'engagent à respecter, en ce qui les concerne, les dispositions du Règlement (UE) 2016-679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

circulation de ces données (RGPD) et celles de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

6.1. Finalités et responsabilités de traitement

Dans le cadre du présent contrat, il convient de distinguer deux traitements de données personnelles et les responsabilités associées, comme suit.

- *Traitement 1 : Traitement de données réalisé pour la conclusion et l'exécution du présent contrat*

Les données personnelles d'identification et les données relatives à l'activité professionnelle des représentants et référents techniques (RSSI) de l'Audité collectées pour la conclusion et l'exécution du présent contrat, font l'objet d'un traitement par l'ANS.

Pour ce traitement, l'ANS agit en qualité de responsable de traitement pour la gestion de l'exécution du présent contrat, ainsi que la gestion du contentieux et du précontentieux.

Tout ou partie de ces données peuvent être transmises aux services internes de l'ANS, ainsi qu'à ses prestataires externes.

Les données personnelles des personnes concernées sont traitées par l'ANS dans le cadre de l'exécution d'une mission d'intérêt public (article 6, 1, (e) du RGPD), à savoir le renforcement de la sécurité des systèmes numériques en santé. Le CERT Santé apporte un appui aux établissements de santé, aux organismes et services exerçant des activités de prévention, de diagnostic ou de soins, ainsi qu'aux établissements et services médico-sociaux dans la réponse à incident de sécurité des systèmes d'information.

- *Traitement 2 : Données personnelles traitées dans le cadre de la réalisation de la Prestation*

Le traitement de données à caractère personnel effectué dans le cadre de la réalisation de la Prestation a pour finalité la détection et l'analyse de potentielles vulnérabilités, l'établissement du rapport d'Audit ainsi que la mise en œuvre de recommandations de remédiation pour améliorer la sécurité du système d'information de l'Audité.

Pour ce traitement, l'Audité agit en qualité de responsable de traitement, et délègue à l'ANS, qui agit en qualité de sous-traitant, la réalisation de la Prestation.

Les données personnelles des personnes concernées sont traitées par l'Audité dans le cadre de l'exécution d'une obligation légale issue du RGPD et du Code de la santé publique (article 6, 1, (c) du RGPD), à savoir d'assurer la sécurité et la confidentialité des données traitées dans le cadre de leur activité.

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

6.2. Catégories de données traitées

Les catégories de données traitées par l'ANS en sa qualité de responsable de traitement pour la conclusion et l'exécution du présent contrat sont les données d'identification et les données relatives à l'activité professionnelle des représentants et référents techniques (RSSI) de l'Audité (nom, prénom, adresse électronique, téléphone, adresse de l'établissement).

Les catégories de données personnelles traitées par l'ANS en sa qualité de sous-traitant dans le cadre de la réalisation de la Prestation sont les suivantes :

- Le périmètre de l'audit indiqué dans la commande initiale (URLs, adresses IP) ;
- Les données à caractère personnel qui auraient fait l'objet d'une exfiltration (identifiants d'accès à un compte) ;
- Les données auxquelles l'ANS pourrait accidentellement accéder dans le cadre des tests d'identifiants réalisés pendant l'exécution de la Prestation (données d'identification, données relatives à l'activité professionnelle, données de santé, etc.) ;

6.3. Obligations de l'ANS en sa qualité de sous-traitant

L'ANS s'engage en sa qualité de sous-traitant à :

- Traiter les données uniquement pour les seules finalités qui font l'objet de la sous-traitance ;
- Traiter les données conformément aux instructions documentées du responsable de traitement. Si le sous-traitant considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en informe immédiatement le responsable de traitement. En outre, si le sous-traitant est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;
- Aider le responsable du traitement à garantir le respect de ses obligations en matière de sécurité, de notification d'une violation de données et de réalisation d'une analyse d'impact relative à la protection des données ;
- Veiller à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
- Mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect de ses obligations en matière de protection des données ;
- Informer préalablement le responsable de traitement de tout transfert de données vers un pays tiers. Les transferts de données à caractère personnel vers un pays tiers ou une organisation internationale sont soumis à un régime spécifique prévu par les articles 44 et suivants du règlement (UE) 2018/1725 ;
- L'ANS peut faire appel à un autre sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques. Le sous-traitant ultérieur est tenu de respecter les obligations de la présente annexe pour le compte et selon les instructions du Responsable de traitement. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

et organisationnelles appropriées pour que le traitement réponde aux exigences du règlement européen sur la protection des données.

6.4. Obligation de l'Audité en sa qualité de responsable de traitement

Outre les autres obligations qui lui incombent en application des présentes, le responsable de traitement s'engage à :

- Documenter par écrit toute instruction concernant le traitement des données par le sous-traitant ;
- Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du sous-traitant ;
- Superviser le traitement ;
- Respecter les obligations qui lui incombent, en sa qualité de responsable de traitement, au regard des dispositions applicables en matière de protection des données à caractère personnel, et tenir indemne l'ANS des conséquences de toute demande, réclamation ou action, de quelque nature qu'elle soit, au titre des obligations lui incombant en sa qualité de responsable de traitement.

6.5. Sécurité et confidentialité des données personnelles

Les Parties mettent en œuvre des mesures organisationnelles, techniques, logicielles et physiques en matière de sécurité du numérique pour protéger les données personnelles contre les altérations, destructions et accès non autorisés.

L'exécution de la Prestation par l'Auditeur peut entrainer un traitement des données à caractère personnel issues des identifiants qui peuvent potentiellement avoir fait l'objet d'une exfiltration et/ou d'une fuite.

L'Auditeur réalise ensuite des tests sur ces identifiants pour révéler l'existence d'une éventuelle vulnérabilité entrainant des accès illégitimes aux comptes des personnes concernées. Dans le cadre de la réalisation de ces tests sur les identifiants, l'ANS peut être amenée accidentellement à accéder à des données à caractère personnel, et notamment des données de santé, lorsque qu'ils permettent effectivement d'ouvrir une session sur laquelle ces données sont accessibles.

Les informations auxquelles l'Auditeur pourrait accidentellement accéder lorsqu'il teste les identifiants ne sont pas conservées. L'Auditeur effectue uniquement une description des vulnérabilités techniques dont l'exploitation permet d'accéder à ces données pour la production du rapport.

L'ensemble des données visées au présent article ne sont pas intégrées au rapport d'audit et ne sont pas transmises à l'Audité.

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

6.6. Violation de données

L'Audité, en sa qualité de responsable de traitement, reste responsable du signalement des incidents graves de sécurité des systèmes d'information prévue à l'article L. 1111-8-2 du code de la santé publique, et du signalement de toute violation de données à caractère personnel au sens du RGPD.

L'ANS en sa qualité de sous-traitant s'engage à informer, dans les meilleurs délais après en avoir pris connaissance, l'Audité de tout incident de sécurité et de toute suspicion de violation de données à caractère personnel telle que définie à l'article 4.12 du RGPD pouvant engendrer un risque pour les personnes concernées, accidentelle ou non.

L'ANS reste responsable de ses obligations en matière de notification de violation de données pour les traitements qu'elle réalise en qualité de responsable de traitement (*Traitement 1*).

6.7. Droits des personnes concernées

Chacune des Parties reste responsable de l'information des personnes relevant de leur périmètre de responsabilité concernant le traitement de leurs données personnelles ainsi que de la mise en place des mesures nécessaires pour garantir les droits des personnes concernées dans les conditions fixées par la législation en vigueur.

- *Information des personnes concernées par le traitement de données réalisé pour la conclusion et l'exécution du présent contrat (Traitement 1)*

Les personnes concernées par le traitement de leurs données à caractère personnel mis en œuvre par l'ANS pour la gestion de la conclusion et l'exécution du présent contrat (Représentant de l'Audité, RSSI, etc.) sont informées qu'elles bénéficient d'un droit d'accès, de rectification et, le cas échéant, d'un droit à la portabilité et à l'effacement de leurs données, ainsi que d'opposition au traitement ou à sa limitation.

Les personnes concernées peuvent exercer leurs droits en adressant une demande :

- par courrier postal, à l'adresse suivante : ANS, Délégué à la Protection des Données, 2-10 Rue d'Oradour-sur-Glane, 75015 Paris ;
- par email à l'adresse dpo@esante.gouv.fr.

Si la personne concernée estime que ses droits n'ont pas été respectés, elle a la possibilité de saisir la Commission Nationale de l'Informatique et des Libertés (CNIL) d'une réclamation

- *Information des personnes concernées par le traitement réalisé dans le cadre de la réalisation de la Prestation (Traitement 2)*

Les personnes concernées par les traitements de données réalisés dans le cadre de la Prestation, seront informées par l'Audité, en sa qualité de responsable de traitement, dans le cadre de l'information faite pour la mise en œuvre des traitements relevant de l'exécution de ses missions.

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

6.8. Durées de conservation

L'Auditeur s'engage à archiver le rapport pour une durée d'un (1) an puis à le supprimer. Les données collectées pour réaliser le rapport sont conservées pendant une durée d'un (1) an après la production de celui-ci.

Les informations auxquelles l'Auditeur pourrait accidentellement accéder lorsqu'il teste les identifiants ne sont pas conservées.

Les données traitées par l'ANS pour la gestion du présent contrat sont conservées pour la durée de la relation contractuelle, sans préjudice des dispositions législatives ou réglementaires propres à certaines catégories de données imposant une durée de conservation particulière ou la suppression de ces données. Aux termes de ces périodes, les données seront archivées de manière sécurisée pour les durées nécessaires de conservation et/ou de prescription résultant des dispositions législatives ou réglementaires applicables.

Dans le cadre de la création de statistiques de suivi, les données seront anonymisées.

7. Communication entre les Parties

De manière générale, les Parties s'engagent à collaborer et à se rapprocher l'une de l'autre pour toute question relative à l'exécution des présentes. Les documents confidentiels seront envoyés chiffrés entre les Parties. Un mot de passe sera communiqué à cet effet.

L'Audité sera destinataire des documents transmis par l'Auditeur.

8. Engagement des Parties

L'Auditeur s'engage pendant toute la durée de la Prestation :

- à réaliser la Prestation avec diligence et compétence ;
- à apporter tout le soin raisonnablement possible à la réalisation de la Prestation confiée par l'Audité ;
- à agir dans le strict cadre méthodologique défini aux présentes et en annexe ;
- à exécuter la Prestation pendant la période de réalisation définie entre les Parties ;
- à prendre toutes les précautions utiles afin de limiter les risques d'endommagement des systèmes d'information audités ;
- à fournir un correspondant disponible pendant toute la durée d'exécution de la Prestation ;
- à avertir l'Audité en cas de découverte d'une anomalie identifiée dans la configuration, l'exploitation ou l'utilisation des systèmes de sécurité, notamment toute éventuelle pratique illicite ;
- à avertir l'Audité en cas de découverture d'une anomalie de criticité majeure ou supérieure ;

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

- à cesser toute action, à la demande de l'Audité, en cas d'impact direct ou indirect sur ses services ;
- à s'assurer que les professionnels exerçant sous sa responsabilité respectent les obligations de confidentialité prévues dans la présente Convention.

L'Audité s'engage pendant toute la durée de la Prestation :

- à fournir des informations exactes concernant les systèmes d'information objet de la Prestation ;
- à fournir un correspondant disponible pendant les heures de travail ouvrées ;
- à donner accès aux systèmes d'information dans le périmètre de la Prestation, selon les modalités définies dans la méthodologie d'audit ;
- à faire un retour d'expérience à l'ANS sur le contenu du rapport, les bénéfices de l'audit et les éventuels points d'amélioration ;
- à s'assurer que l'environnement technique permet de réaliser la Prestation sur le système d'information cible en toute sécurité et effectuer toutes les sauvegardes nécessaires ;
- le cas échéant à disposer de toutes les autorisations nécessaires à la réalisation de la Prestation dans les conditions du présent Protocole, notamment l'autorisation des utilisateurs des éléments cibles du périmètre de la Prestation, et des éventuels tiers ayant droit sur lesdits éléments cibles ;
- à ne solliciter l'Auditeur que dans le périmètre et dans le respect de la méthodologie précisée en annexe du Protocole.

L'ensemble des Parties s'engagent à ce que la Prestation soit réalisée conformément à la réglementation en vigueur et aux conditions du présent Protocole.

9. Modalités financières

La Convention est conclue à titre gracieux.

10. Responsabilités

La responsabilité des Parties pourra être recherchée en cas de non-respect des dispositions du présent Protocole.
L'Audité reconnaît et accepte que les méthodologies utilisées pour réaliser la Prestation ne sauraient garantir l'identification exhaustive de toutes les failles de sécurité.

11. Durée et date d'effet du protocole

La présente Convention prend effet à la date de sa signature par la dernière des Parties, et restera en vigueur jusqu'à la date de remise du rapport définitif par l'Auditeur à l'Audité.

Les stipulations de l'article 5 relatives à la confidentialité survivront à l'extinction de la présente Convention, et ce pendant une durée de (5) ans au-delà de la fin de la présente Convention.

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

12. Fin anticipée de la Convention

12.1. Résiliation

La Convention peut être résiliée à tout moment par l'une des Parties, dans le respect d'un délai de trente (30) jours à compter de la réception d'une lettre recommandée avec accusé de réception notifiant le souhait de cette Partie de mettre fin à la Convention.

12.2. Manquement d'une Partie à ses engagements

Dans l'hypothèse où l'une des Parties manquerait à une obligation lui incombant au titre de la Convention, les Parties cherchent à résoudre amiablement la situation qui en découle, sous trente (30) jours à compter de la réception d'un courrier avec avis de réception faisant état du manquement.

A défaut de résolution amiable dans ce délai, la Partie la plus diligente peut mettre fin à la Convention dans les conditions de l'article 12.1 de la Convention ou saisir la juridiction visée à l'article 13 de la Convention.

13. Loi applicable et tribunaux compétents

La présente Convention est soumise au droit français. En cas de litige qui viendrait à naître entre les Parties à propos de l'exécution ou de l'interprétation des présentes, les Parties s'engagent en tout premier lieu à coopérer avec diligence et bonne foi afin de rechercher une solution amiable. A défaut d'accord amiable constaté par la Partie la plus diligente, tout litige résultant de l'application de la présente convention relèvera de la compétence des tribunaux du ressort de Paris.

14. Signature électronique

En signant, les Parties reconnaissent que la Convention signée électroniquement constitue un document original et que la force probante de la signature électronique est assimilable à celle d'une signature réalisée par écrit.

En outre, les Parties reconnaissent que le processus de signature électronique et le dossier de preuve généré automatiquement constituent des éléments de preuve recevables.

Une fois la Convention signée par l'ANS, le représentant légal de l'Audité reçoit par courrier électronique, à l'adresse renseignée sur la plateforme Cybersurveillance, une invitation à signer la présente Convention via la plateforme YouSign. Le processus de signature de l'Audité se déroule comme suit :

- Le représentant légal de l'Audité reçoit un courrier électronique contenant un lien sécurisé vers la plateforme YouSign ;
- Il consulte la convention présignée par l'ANS directement dans son navigateur, sans nécessité d'installation de logiciel ;

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

- Il procède à la signature en confirmant son identité via un code à usage unique (OTP) transmis par SMS sur le numéro de téléphone renseigné lors de sa demande d'audit ;
- Un exemplaire de la Convention signée par les deux Parties est automatiquement adressé à l'Audité par courrier électronique.

La signature de la présente convention est un prérequis à la réalisation de la Prestation.

Pour l'Auditeur	Pour l'Audité

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

ANNEXE : DETAIL DE LA PRESTATION

La méthodologie, le périmètre, le détail des tests ainsi que les prérequis retenus par l'Auditeur et validés par l'Audité sont précisés de manière exhaustive dans la présente annexe.

La présente annexe doit être complétée avant la signature de la Convention.

I. Méthodologie

L'approche méthodologique retenue pour la Prestation est la suivante :

Les différentes phases :

Phase 1 : Récupération d'informations

Cette étape consiste à collecter toutes sortes d'informations techniques sur la cible :

- De manière publique :
  - à partir des sites référençant le domaine surveillé ;
  - à partir de recherches Google customisées (Google Dork, GoolaG) ;
  - à partir d'informations se trouvant dans des forums ou des groupes de discussion ;
  - à partir des informations des sites du domaine audité ;
  - à partir des informations publiques de noms de domaines et d'hébergement.
- De manière « osée » :
  - en envoyant des requêtes « spéciales » (transfert de zone DNS, requêtes de bannières, etc.) ;
  - en testant les services ouverts (WWW, Mail, FTP, News, LDAP, etc.) ;
  - en étudiant le code source des pages des sites Web ;
  - en utilisant des particularités protocolaires réseaux (divers traceroute, ping avec options, etc.).
- De manière « ciblée » :
  - en utilisant des scanners de ports TCP/UDP ;
  - en utilisant des scanners applicatifs (http, FTP, etc.) ;
  - en utilisant des outils réseaux spécifiques (Nessus, Whisker, nikto, etc…).

Cela permet de déterminer un premier niveau de cartographie des services et ressources Internet à auditer.

Phase 2 : Analyse des informations recueillies

Le but de cette étape est d'identifier le plus précisément possible les services ouverts sur Internet (messagerie, DNS, serveur FTP, serveur Web, VPN, etc.), les serveurs hébergeant ces services, les versions de logiciel installées sur ces serveurs.

Après l'établissement de la « cartographie », une recherche de toutes les vulnérabilités potentielles liées à chaque service en ligne est réalisée.

Les recherches sont réalisées au moyen :

- des services publics de référencement Internet (AFNIC, RIPE, INTERNIC, etc.) ;

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

- des services de forums/newsgroups ;
- des informations fournies par les serveurs Web ;
- pour les CMS, des composants (plugins, thèmes, widget…) utilisés pour identifier le type et la version (Wordpress, Drupal, EZpublish…) ;
- des outils de scan de ports (Nmap, Superscan, etc.) ;
- des scanners de vulnérabilités généraux ou spécifiques (Nessus, Nikto, etc.) ;
- des outils propriétaires développés sur mesure pour ce type d'audit de sécurité.

Les tests permettent notamment d'identifier :

- des vulnérabilités en conception (conception du produit ou du protocole) ;
- des vulnérabilités en exploitation (configuration du produit, utilisation).

Aucun test agressif (débordement de tampon mémoire, dénis de service, exploitation d'une vulnérabilité, test de la robustesse de mots de passe) n'est effectué dans le cadre de l'audit.

Néanmoins dans certains cas particuliers et sous réserve de l'autorisation préalable de la structure, l'ANS a le droit d'exploiter certaines vulnérabilités afin d'établir une liste de ses potentiels impacts.

II. PLANNING ET CONTACT

Les tests seront réalisés entre le ……/…../……. Et le ……/…../……. (inclus).

Ces durées pourront être modifiées moyennant l'accord commun des Parties, formalisé par un avenant au présent Protocole.

Les points de contact, pour chacun des Parties, sont les suivants :

- Contacts de l'ANS : cybersurveillance@esante.gouv.fr et cyberveille@esante.gouv.fr

- Contact de l'Audité : ……

III. Périmètre

Le périmètre de l'audit est le suivant :

Périmètre de l'audit à compléter par l'Audité	
Nom des domaines concernés	

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.

Nom des domaines infogérés	
Les adresses IP concernées	
Les adresses IP infogérées	
Les adresse IPs utilisées pour les tests	

IV. Prérequis

Afin de réaliser les tests d'intrusion, la communication des éléments suivants sera nécessaire :

- Choix d'une date d'audit en fonction des disponibilités ;
- Scan des domaines/sous-domaines de l'ES et sélection du périmètre à auditer ;
- Mise en liste blanche des IP de test si possible pour eux ;
- Convention à signer et envoyer à l'ANS ;

V. Précautions particulières

Afin de limiter les effets liés à la réalisation des tests présentés, les précautions suivantes seront mises en œuvre :

Aucune attaque de type déni de service par surcharge du trafic réseau ne sera menée.

Aucune attaque de type débordement de zone tampon ne sera délibérément réalisée.

Les tests réalisés seront réalisés depuis les locaux de l'ANS depuis les adresses IP suivantes :

- 195.15.130.154
- 51.254.157.247

Cependant, la réalisation de tests d'intrusion comporte toujours un risque d'altération du service, la découverte d'une vulnérabilité étant très souvent liée à son exploitation. Dans ce cadre, il est important de prévenir rapidement les contacts mentionnés dans ce présent protocole afin de réagir rapidement en cas d'incident.

Ce document est la propriété de l'ANS - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ANS sont interdites.