



REPUBLIQUE FRANCAISE
Département des Pyrénées Orientales
COMMUNAUTE DE COMMUNES
ALBERES COTE VERMEILLE ILLIBERIS

N° DC2024-0078

D É C I S I O N

Portant contrat de maintenance des équipements et contrat d'expertise Firewall 100F, et le maintien en conditions opérationnelles des infrastructures Fortinet pour les sites de la CC ACVI

CC ACVI / SNS SECURITY

Le Président de la Communauté de Communes Albères Côte Vermeille Illibérus,

Vu le Code Général des collectivités territoriales et notamment son article L 5211.10,

Vu la délibération n°DL2020-0202 du Conseil Communautaire en date du 31/07/2020 portant délégation d'attributions de l'organe délibérant au Président pour les actes relatifs aux conventions, contrats de maintenance et d'entretien des matériels et licences informatiques (logiciels, photocopieurs, ascenseurs, téléphone...),

Considérant la nécessité de recourir à un prestataire extérieur pour le contrat de maintenance des équipements et contrat d'expertise Firewall 100F, et le maintien en conditions opérationnelles des infrastructures Fortinet pour les sites de la CC ACVI,

Considérant les termes de la proposition du contrat de maintenance des équipements et contrat d'expertise Firewall 100F, et le maintien en conditions opérationnelles des infrastructures Fortinet pour les sites de la CC ACVI passée entre la CC ACVI société SNS SECURITY dont le siège social est situé 381 Avenue du Mas d'Argelliers-Bat le New Work 1 ETG 2-MONTPELLIER (34 070), SIRET 442 364 352 00074 et représentée par Monsieur Yacine HAMZAoui, son commercial,

Considérant que le contrat est conclu pour une durée de trois ans à partir du 30 juin 2024,

DECIDE

ARTICLE 1 : D'APPROUVER le contrat de maintenance des équipements et contrat d'expertise Firewall 100F, et le maintien en conditions opérationnelles des infrastructures Fortinet pour les sites de la CC ACVI, passé entre la CC ACVI et la société SNS SECURITY dont le siège social est situé 381 Avenue du Mas d'Argelliers-Bat le New Work 1 ETG 2-MONTPELLIER (34 070), SIRET 442 364 352 00074,

ARTICLE 2 : D'INDIQUER que les prestations décrites dans le présent contrat sont déterminées pour la période totale sur la base d'un montant de rémunération de 5 480.00-€ HT (cinq mille quatre cent quatre-vingt euros hors taxes – TVA en vigueur en sus),

ARTICLE 3 : DE PRECISER que le prix des prestations fera l'objet d'une révision annuelle selon les conditions mentionnées dans l'article 21.2 du présent contrat,

Accusé de réception en préfecture
066-200043602-20240507-DC2024-0078-AR
Date de télétransmission : 07/05/2024
Date de réception préfecture : 07/05/2024

ARTICLE 4 : DE PRECISER que le renouvellement de ce contrat est conclu pour une durée de 3 ans à compter du 30 juin 2024 avec une fin au 30 juin 2027,

ARTICLE 4 : DE SIGNER toutes les pièces relatives à ce dossier,

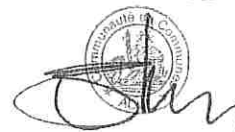
ARTICLE 5 : DE PRECISER qu'il sera rendu compte lors de la prochaine réunion du Conseil Communautaire de la présente décision.

Fait à Argelès-sur-Mer, le 07/05/2024,

Pour extrait certifié conforme et exécutoire, du
fait de sa publication et sa transmission en
Préfecture
Le président

Antoine PARRA

Pour le Président par délégation
Le Directeur Général des Services
Henri ESTEVE

A circular official stamp of the Argelès-sur-Mer Communauté is partially visible behind a handwritten signature in black ink.

Le présent acte peut faire l'objet d'un recours devant le Tribunal Administratif de Montpellier dans un délai de deux mois à compter de la date à laquelle il est devenu exécutoire.

Date du document : 17/01/2024
Date de validité : 1 mois
Nos références : CTT_100F_3A_DC
Vos références :
Commercial : YACINE HAMZAQUI

Page 1

N° SIRET : 20004360200016

Adresse de livraison

COMMUNAUTE DES COMMUNES ALBERES COT

ROGER CARRERE

CHEMIN DE CHARLEMAGNE

66704 ARGELES SUR MER CEDEX

Adresse de facturation

CCACV - COMMUNAUTE DE COMMUNES ALBERES COTE

CHEMIN DE CHARLEMAGNE

66704 ARGELES SUR MER CEDEX

Désignation	PU HT	Remise	PU Net	Qte	Total HT
RENEW CTT FIREWALL 100F DATA CENTER - CC COTE VERMEILLE					
[S] SECURE - CONTRAT D'EXPERTISE FIREWALL FORTIGATE 3 ANS MAINTIEN EN CONDITIONS OPERATIONNELLES DE VOS INFRASTRUCTURES FORTINET	8 100,00	20%	6 480,00	1,00	6 480,00
Partenaire historique de FORTINET en France, SNS SECURITY s'appuie sur l'expertise de ses ingénieurs certifiés NSE4/NSE5/NSE6/NSE7 pour assurer la sécurité de votre patrimoine informationnel. Conseil, intégration, confiez-nous aussi la supervision de vos équipements : FORTIGATE, FORTIWEB, FORTIMAIL, ...					
• Exploitation ou cogérance de votre matériel FORTIGATE. • Accès illimité à notre support technique d'ingénieurs certifiés. • Support téléphonique direct (sans filtrage ni sélection) 5j/7 de 8h à 18h. • Aide à la mise en place d'une politique de durcissement de votre système d'information. • Recommandations sur l'évolution de votre système d'information conformément aux bonnes pratiques de l'ANSSI. • Mise à niveau de vos dispositifs de sécurité, gestion des correctifs et mise en place des nouvelles fonctionnalités. • Toute demande de changement excédent 1j, pourra être sujet à une évaluation tarifaire. • Maintenance curative : résolution des incidents. • Monitoring de vos liens WAN et gestion des tickets opérateurs a la demande. • Remplacement en j+1 pour les pare-feux, point d'accès Wi-Fi en cas de panne.					
*** Contrat: 30/06/2024 --> 30/06/2027 ***					
REMISE EXCEPTIONNELLE SSECURE	-1 000,00		-1 000,00	1,00	-1 000,00

Nom, date, tampon et signature *

* avec mention "Bon pour accord" pour le Président par délégation Le Directeur Général des Services Henri ESTEVE devis valable 1 mois

« Je déclare avoir pris connaissance des conditions générales disponibles sur notre site web : <https://www.sns-security.fr/CGV> et les accepter dans leur intégralité »

Récapitulatif

Total Net HT :	5 480,00 €
TVA 20% :	1 096,00 €
Total TTC :	6 576,00 €
Acompte versé :	0,00 €
NET A PAYER :	6 576,00 €

Document libellé en : Euro

Condition de règlement : VIREMENT A 30 JRS NETS

Nos coordonnées bancaires : CREDIT AGRICOLE - IBAN : FR76 1350 6100 0085 1068 7031 078 - BIC/SWIFT : AGRIFRPP835

Dans le cadre d'une offre locale, d'un abonnement XDSL / fibre optique, service antispam, le paiement est uniquement par prélèvement. Toute commande ne sera validée qu'à réception des éléments complémentaires à savoir un mandat SEPA dûment signé accompagné d'un RIB. Nous nous réservons la propriété des matériels et fournitures jusqu'au paiement complet du prix par l'acheteur. Notre réserve de propriété porte aussi bien sur les marchandises que sur les prix si elles ont déjà été revendues (loi N°8.335 du 12 Mai 1980).

5 ENTREE EN VIGUEUR - DUREE

5.1 Entrée en vigueur

Le Contrat entre en vigueur à compter de la signature du Bon de commande et de l'acceptation des présentes, des éventuelles Conditions Particulières et Conditions Spécifiques par le Client, et le cas échéant, encaissement de l'acompte prévu.

5.2 Durée

Le Contrat est à durée déterminée telle que mentionnée sur le Bon de commande et calculée à compter de la Date de Mise à disposition, déterminée comme suit :

- la date de Recette du Service ;
- la date de l'envoi du Matériel et/ou de la mise à disposition du Logiciel au Client.

Si le Matériel n'a pas été envoyé dans un délai raisonnable du fait de la non-disponibilité du Client, la Date de Mise à disposition sera automatiquement réputée être 90 jours après la date de signature du Bon de Commande.

Différentes durées peuvent s'appliquer à différents Services. Les Services proposés peuvent faire l'objet de Périodes Minimales d'engagement. Ces durées et Périodes Minimales sont indiquées sur le Bon de Commande.

Au terme de sa Période Minimale, chaque Service peut être renouvelé tacitement pour une durée indéterminée ou pour de nouvelles Périodes Minimales d'engagement successives.

Les Parties conviennent, sauf dérogation précisée dans les Conditions Particulières ou Conditions Spécifiques, que le Contrat, concernant une Location ou un abonnement de lien d'accès à internet se renouvellera ensuite, pour une période de 12 mois reconductible par tacite reconduction sauf dénonciation de l'une des Parties dans les conditions de l'article « Résiliation pour convenance » ci-après.

6 ANNULATION DES SERVICES, VENTES OU LOCATION

En cas d'annulation des Services, ventes ou Locations souscrits par le Client après acceptation du Bon de commande pour quelque raison que ce soit hormis la force majeure, l'acompte versé à la commande sera de plein droit acquis à SNS SECURITY et ne pourra donner lieu à un quelconque remboursement.

De surcroît, SNS SECURITY pourra, discrétionnairement, décider de facturer la totalité des Services, ventes ou Locations annulés ou décider de facturer les frais engagés, par elle le tout de plein droit et sans aucune formalité préalable obligatoire.

7 OFFRE D'EQUIPEMENTS ET DE SERVICES

7.1 Caractéristiques des Equipements et des Services

Les caractéristiques des Equipements et Services pourront être définies dans un catalogue. Le catalogue fourni pourra être le catalogue de SNS SECURITY ou d'un Fournisseur.

SNS SECURITY communique au Client l'ensemble des caractéristiques des Equipements et/ou Service notamment le descriptif, les spécifications et le prix.

SNS SECURITY se réserve le droit de supprimer et/ou modifier les Equipements et Services qu'elle propose dès qu'elle le jugera utile afin de s'adapter au marché.

Les Equipements ou Services sont conformes aux normes françaises. Pour les Equipements et Services à destination de l'étranger, le Client s'engage à vérifier que ces Equipements et Services répondent aux normes en vigueur dans le pays du lieu de livraison ou d'exécution.

7.2 Disponibilité des Equipements

L'offre des Equipements est valable dans la limite des stocks disponibles auprès du Fournisseur.

En cas d'éventuelle rupture de stocks affectant la commande en cours, SNS SECURITY indiquera dans les meilleurs délais et par tous moyens au Client un nouveau délai de livraison.

Dans ce cas, SNS SECURITY aura la possibilité de proposer au Client un Equipement de remplacement, ayant au moins les mêmes caractéristiques techniques.

Dans l'hypothèse où un Equipement serait indisponible, SNS SECURITY peut livrer au Client un autre Equipement de qualité et de prix équivalents ou supérieurs à celui initialement commandé, sous réserve de l'accord exprès du Client. Un changement de référence ou le remplacement par le Fournisseur d'un Equipement par un autre Equipement de qualité équivalente ou

supérieure, n'est pas soumis à l'accord du Client, dès lors que le prix reste inchangé.

Le Client reconnaît et accepte que les situations précitées sont inhérentes aux cycles technologiques et commerciaux et contraintes de production des Equipements, et ne sont pas de nature à lui permettre de solliciter des dommages et intérêts.

8 INSTALLATION ET MISE EN SERVICE

8.1 Informations préalables

Le Client s'engage à communiquer à SNS SECURITY toutes les informations et documentations demandées par SNS SECURITY et nécessaires à la mise en œuvre du Bon de Commande et à l'exécution du Contrat, par exemple, à la configuration nécessaire des Equipements SNS SECURITY.

Le Client s'engage pour cela à maintenir une collaboration active et régulière en remettant à SNS SECURITY l'ensemble des éléments demandés, notamment le Contenu.

Pour sa part, SNS SECURITY s'engage à communiquer toutes les difficultés dont elle pourrait prendre la mesure, au regard de son expérience, au fur et à mesure de l'exécution du Contrat, afin de permettre leur prise en compte le plus rapidement possible, participant ainsi à la réussite de l'ensemble des Services prévus au présent Contrat.

Le Client s'engage à tenir SNS SECURITY informée des actions effectuées dans le cadre d'activités ne relevant pas du présent Contrat qui seraient susceptibles d'avoir une incidence sur son exécution.

Le Client est et demeure seul propriétaire des Contenus, documents, des données, des informations et fichiers qui pourraient être communiqués à SNS SECURITY pour les besoins des présentes ou auxquels SNS SECURITY pourrait avoir accès dans le cadre de l'exécution des présentes. A charge pour le Client de s'assurer qu'il est en droit de lui communiquer ces éléments.

La responsabilité de SNS SECURITY ne peut être engagée en cas d'informations erronées ou incomplètes fournies par le Client à SNS SECURITY.

SNS SECURITY, au-delà du périmètre d'exécution du Contrat, peut être amenée, sans que cela constitue une obligation à sa charge, à adresser des alertes et des mises en garde sur des problématiques de sécurité notamment en matière de Matériels et de Logiciels. A réception de l'information, il appartient au Client de prendre les toutes dispositions en conséquence sous sa seule et unique responsabilité.

8.2 Recette du Service

Le Client reçoit de SNS SECURITY par tout moyen un avis de mise à disposition du Service selon le type de Service commandé.

Cet avis contient la date à laquelle le Service est ou sera opérationnel.

A compter de cette date, le Client est invité par SNS SECURITY à vérifier la conformité du Service avec les spécifications figurant au Bon de Commande, et ce, dans un délai maximal de 7 jours calendaires pour faire part, par écrit, à SNS SECURITY de ses éventuelles réserves. A défaut de réserves notifiées dans ces formes et délai, le Client est réputé avoir tacitement accepté le Service. Toute demande ultérieure relative à la correction d'Incidents éventuels est traitée dans le cadre de la maintenance effectuée par le Support Technique.

Les éventuelles réserves sont notifiées à SNS SECURITY par écrit. SNS SECURITY informe alors le Client de la date prévisionnelle de levée de ces réserves. Une fois les réserves levées par SNS SECURITY, le Client reçoit un nouvel avis de mise à disposition du Services ouvrant une nouvelle période de Recette de 7 jours calendaires. Cette Recette est limitée à la vérification de la correction des seules anomalies identifiées lors de la première période de Recette.

Si les réserves ne sont pas levées au deuxième ajournement, de nouvelles procédures de Recette seront réalisées selon les conditions décrites ci-avant jusqu'à leur levée.

Seule la Recette sans réserve ou la Recette tacite à l'expiration de l'un ou l'autre des délais de 7 jours précités vaut Recette du Service.

9 LIVRAISON DES EQUIPEMENTS

9.1 Livraison

Les délais indicatifs de livraison des Matériels et de mise à disposition des Logiciels sont précisés sur le Bon de Commande. Cependant, en fonction du nombre et du type de Matériel et/ou de Logiciel, SNS SECURITY pourra

1 DEFINITIONS

Les termes ci-dessous définis ont entre les Parties la signification suivante :

- **Bon de Commande** : désigne le document détaillant les modalités d'exécution des Services commandés par le Client, il peut être présenté sous forme de devis accepté par le Client ou par un bon de commande ;
- **Client** : désigne la personne morale, identifiée dans le Bon de Commande, bénéficiaire du (des) Service(s), de la Location ou de la vente d'Equipements pour ses besoins professionnels au titre du Contrat ;
- **Conditions Générales** : désigne le présent document ;
- **Conditions Particulières** : désigne les Conditions Particulières afférentes à chaque Service fourni par SNS SECURITY et complétant les présentes Conditions Générales ;
- **Conditions Spécifiques** : désigne conditions complémentaires ou déroatoires aux Conditions Générales de Vente et/ou Conditions Particulières dans lesquelles SNS SECURITY propose au Client ses Services. Elles portent sur les aspects spécifiques techniques ou réglementaires des Services souscrits par le Client ;
- **Consommation** : désigne toute utilisation du Service calculée et facturée en fonction du volume consommé ou acheté par le Client ;
- **Contenu** : désigne les informations, messages, données ou communications échangées par l'intermédiaire du Service ;
- **Contrat** : désigne l'ensemble contractuel comprenant les documents énumérés à l'article « Documents Contractuels » ;
- **Cybersécurité** : désigne les mesures techniques, organisationnelles et juridiques ayant pour objet de protéger les Equipements, les systèmes informatiques, les données et les informations contre les menaces et les attaques malveillantes ;
- **Date de Mise à disposition** : désigne la date constituant le point de départ de la fourniture effective d'un Service ou d'un Equipement par SNS SECURITY, ainsi que sa facturation, telle que définie à l'article « Durée » des présentes ;
- **Données Personnelles** : désignent les données qui, au sens du règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, permettent de désigner ou d'identifier, directement ou indirectement, une personne physique ;
- **Equipements** : désigne les Matériels et Logiciels du Client et/ou de SNS SECURITY, utilisés pour la fourniture du Service ou faisant l'objet d'une Location ou d'une vente ;
- **Equipements Client** : désigne les Matériels et Logiciels du Client, y compris ceux achetés par le Client auprès de SNS SECURITY ou faisant l'objet d'une Location ;
- **Equipements SNS SECURITY** : désigne les Matériels et Logiciels appartenant à SNS SECURITY, mis à disposition du Client par SNS SECURITY dans le cadre de la fourniture du Service, tels que décrits dans le Bon de Commande ;
- **Fournisseur** : désigne l'entité qui conçoit, produit ou assemble un Equipement ou qui édite un Logiciel. Le Fournisseur est responsable des dommages causés par des défauts de fabrication, de conception ou d'avertissement liés à ses Equipements. Le Fournisseur peut détenir les droits de propriété intellectuelle sur l'Equipement, ou bénéficier d'une licence de la part du titulaire des droits. Le distributeur de ces Equipements est assimilé dans les présentes au Fournisseur ;
- **Incident** : désigne tout dysfonctionnement reproductible emportant une interruption totale ou importante dégradation du Service ou de l'Equipement impliquant un risque notable quant à la sécurité du système d'information du Client, alors que le Service ou l'Equipement est utilisé conformément aux instructions de SNS SECURITY ;
- **Jour Ouvré/Heure Ouvrée** : désigne un jour normalement travaillé généralement du lundi au vendredi de 08h00 à 18h00 hors jour férié français ;
- **Location** : désigne la mise à disposition payante d'un Matériel et/ou d'un Logiciel et/ou d'un Service y étant associé par SNS SECURITY au profit du Client ;

- **Logiciels** : désigne les programmes et Virtual Machine (VM), ainsi que la documentation associée, édités par des Fournisseurs et proposés par SNS SECURITY au Client ;
- **Matériel** : désigne les matériels physiques ou tangibles, qui peuvent être vendus par SNS SECURITY ou faire l'objet d'une Location au profit du Client ;
- **Partie(s)** : désigne au singulier SNS SECURITY ou le Client et au pluriel SNS SECURITY et le Client ;
- **Période Minimale** : désigne la durée déterminée et ferme d'engagement du Client au titre d'un ou plusieurs Services, commençant à courir à la Date de Mise à disposition du Service ;
- **Recette** : désigne la procédure de vérification de conformité du Service par le Client décrit à l'article « Recette de Service » ;
- **Service(s)** : désigne-le ou les services fournis par SNS SECURITY au titre du Contrat tels qu'identifiés dans un ou plusieurs Bon(s) de Commande. A chaque Service peuvent être associées des Conditions Particulières et, le cas échéant, des Conditions Spécifiques ;
- **Support Technique** : désigne le Service d'assistance technique délivré par SNS SECURITY au Client afin de résoudre les Incidents ou de répondre à des questions liées à un Service délivré par SNS SECURITY.

2 OBJET

Les présentes Conditions Générales ont pour objet de définir les termes et conditions de fourniture des Services commandés par le Client à SERVICES NETWORK SECURITY SAS située 381 du Mas d'Argelliers, bâtiment Le New Work 1, étage 2, à MONTPELLIER 34070, immatriculée sous le n° 442 364 352 RCS MONTPELLIER (« SNS SECURITY »).

En sus des Services, SNS SECURITY propose la vente ou la Location d'Equipements au Client.

Selon le cas, le Client pourra être amené à accepter les conditions générales du Fournisseur de l'Equipement tels que notamment FORTINET, SentinelOne, Sekoia ou encore Wallix ainsi que les conditions générales de l'opérateur principal dans le cadre de la fourniture de liens opérateurs en marque blanche.

3 DOCUMENTS CONTRACTUELS

Les présentes Conditions Générales constituent la base juridique commune à l'ensemble des Services commandés par le Client à SNS SECURITY ainsi qu'à la vente et la Location d'Equipements. Ces Conditions Générales sont complétées par un ou plusieurs Bon(s) de Commande, des Conditions Particulières propres aux Services choisis par le Client et, le cas échéant, des Conditions Spécifiques.

Le Contrat est constitué par l'ensemble des documents contractuels suivants présentés par ordre hiérarchique de valeur juridique décroissante, à l'exclusion de tous autres documents :

- le ou les Bons de Commande et les annexes éventuelles ;
- les Conditions Spécifiques ;
- les Conditions Particulières ;
- les Conditions Générales.

En cas de contradiction entre une ou plusieurs stipulations figurant dans l'un quelconque des documents ci-dessus, les stipulations contenues dans le document de rang hiérarchique supérieur prévalent.

4 INDEPENDANCE

Les différents Services listés dans le(s) Bon(s) de Commande sont indépendants les uns des autres. En cas de difficultés d'exécution, d'inexécution ou de résiliation de Services, les Parties conviennent que cela sera sans incidence sur les autres Services, leurs Conditions Particulières, Conditions Spécifiques et les présentes Conditions Générales.

La résiliation de l'ensemble des Services entraînera la résiliation du Contrat dans son intégralité.

modifier le délai indicatif mentionné sur le Bon de Commande et préviendra à cet effet le Client dans les meilleurs délais selon tous moyens à sa convenance.

D'une manière générale, SNS SECURITY fera tout son possible pour informer, selon tous moyens à sa convenance, le Client de la date :

- de départ de son colis pour le Matériel ;
- de mise à disposition du Logiciel.

Dans tous les cas, si le jour de livraison et/ou de mise à disposition coïncide avec un jour férié, un jour chômé ou un dimanche, la livraison et/ou la mise à disposition s'effectuera le premier Jour Ouvré suivant.

Les délais ne sont mentionnés qu'à titre indicatifs de telle sorte que SNS SECURITY ne pourra voir sa responsabilité engagée à l'égard du Client en cas de retard de livraison et/ou de mise à disposition. Conséquemment, le Client, en cas de dépassement des délais de livraison ou de mise à disposition, renonce expressément à toute remise, pénalité de retard, dommages et intérêts, ou annulation des commandes en cours.

La livraison du Matériel est réalisée, à défaut d'indication contraire sur le Bon de Commande, à l'adresse du Client figurant sur le Bon de Commande.

La mise à disposition du Logiciel s'effectuera par l'envoi d'un lien à l'adresse e-mail indiquée par le Client sur le Bon de Commande ou par téléchargement du Logiciel directement sur le site internet du Fournisseur en respectant les conditions fixées par ce dernier.

SNS SECURITY ne pourra voir sa responsabilité engagée du fait notamment de la non-conformité d'une adresse postale de livraison et/ou adresse e-mail communiquée par un Client ou en cas d'impossibilité d'accéder au site internet du Fournisseur pour le téléchargement du Logiciel.

Le Client déclare bien connaître le Matériel objet de la Location ou de l'achat et/ou le Logiciel fourni et accepte de les prendre dans l'état dans lequel ils se trouvent, reconnaissant qu'ils sont effectivement propres à leur usage.

Les livraisons hors France métropolitaine sont soumises à des conditions particulières disponibles sur demande.

9.2 Transfert des risques sur les Matériels

Le risque de perte et de détérioration sera transféré au Client dès la réception du Matériel au Client. Le Client s'oblige, en conséquence, à faire assurer dès la commande, à ses frais, les Matériels commandés par une assurance ad hoc, jusqu'au complet transfert de propriété et à en justifier à ce dernier lors de la livraison. A défaut, SNS SECURITY serait en droit de retarder la livraison jusqu'à la présentation de ce justificatif.

Les frais et risques de transport sont à la charge du Client sauf dérogation prévue dans le Bon de Commande.

En conséquence, le Client renonce à tout recours contre SNS SECURITY en cas de perte, de disparition ou, d'une manière générale, pour tout dommage subi par le Matériel après la réception.

Dès la livraison, il appartient au Client :

- de vérifier le bon état, la conformité aux spécifications demandées et la quantité des Matériels reçus ;
- de signer le bon de livraison du transporteur ;
- de recourir, le cas échéant, aux procédures prévues par les articles L. 133-3 et suivants du Code de commerce auprès du transporteur en émettant toutes réserves précises et motivées sur le titre de transport et en confirmant ces réserves par lettre recommandée avec accusé de réception dans un délai de trois (3) jours (dimanche et jours fériés français exclus) à compter de la date de livraison. Le Client s'engage à communiquer simultanément à SNS SECURITY la copie de ladite lettre de réserves. Le défaut de notification des réserves dans les délais et formes ci-dessus, éteint tout recours du Client à l'encontre du transporteur et de SNS SECURITY, les Matériels étant alors considérés comme acceptés en l'état par le Client.

Tout retour de Matériel doit faire l'objet d'un accord préalable de SNS SECURITY. En cas d'acceptation de la réclamation, les Matériels seront retournés par le Client dûment emballés accompagnés de la facture et du bordereau de livraison. Le cas échéant, le Client s'engage à prendre en charge les frais de transport de retour.

En outre, lorsque le Client refuse de réceptionner les Matériels commandés, SNS SECURITY sera en droit de remettre les Matériels en entrepôt aux frais du Client et de lui réclamer le remboursement des frais de transport et d'entreposage.

9.3 Transfert de propriété des Matériels

Le transfert de propriété de tout Matériel vendu par SNS SECURITY au Client est subordonné au paiement complet du prix par ce dernier.

Le Client s'interdit d'en disposer et d'en conférer des droits à des tiers, à titre onéreux ou gratuit, sous quelque forme que ce soit, avant leur complet paiement, sous réserve d'une autorisation expresse et préalable de SNS SECURITY. Si les Equipements objets de la réserve de propriété ont été revendus par le Client, la créance de SNS SECURITY sera automatiquement reportée sur la créance du prix des Equipements vendus.

Dans le cas où le paiement du prix n'interviendrait pas dans le délai prévu au Bon de Commande ou, à défaut, dans les présentes Conditions Générales, SNS SECURITY se réserve le droit de reprendre le Matériel livré. Ils devront être restitués à SNS SECURITY en parfait état de fonctionnement à première demande.

10 INSTALLATION DES EQUIPEMENTS

Sauf difficultés, SNS SECURITY met en œuvre les moyens nécessaires et prend en charge tout ou partie des frais d'installation des Equipements. En cas de difficultés non prévus dans le Bon de Commande, les frais supplémentaires à engager sont à la charge du Client sur la base d'un devis préalable transmis par SNS SECURITY dont l'acceptation par le Client conditionnera la réalisation des opérations nécessaires à l'installation des Equipements.

L'installation des Equipements sera réalisée aux conditions fixées dans le Bon de Commande.

La responsabilité de SNS SECURITY ne saurait être recherchée ou engagée pour tout litige qui opposerait le Client à des tiers à propos des opérations d'installation des Equipements.

Le Client s'engage à n'utiliser que des terminaux agréés et des Equipements compatibles avec les normes et standards de sécurité et de télécommunication. Le Client s'assure que ses Equipements Clients, non installés par SNS SECURITY, sont parfaitement configurés et dimensionnés.

Sur demande du Client, comme indiqué sur le Bon de Commande, SNS SECURITY procédera à l'installation et/ou à la configuration des Equipements.

L'installation et/ou la configuration pourra se faire sur place ou à distance.

SNS SECURITY déterminera en commun accord avec le Client les jours et heures d'installation et/ou de configuration étant précisé que ce sera obligatoirement un Jour Ouvré et à une Heure Ouvrée.

A cet effet, un courriel de confirmation sera adressé au Client.

SNS SECURITY se réserve le droit de sous-traiter l'installation et/ou la configuration des Equipements, ce que le Client reconnaît et accepte.

SNS SECURITY fera toutes diligences et apportera tous les soins nécessaires à la bonne exécution de l'installation et/ou de la configuration des Equipements.

Le Client s'engage à laisser à SNS SECURITY, à ses salariés et à ses sous-traitants le libre accès à ses locaux et à ses Equipements Clients, que l'intervention soit réalisée sur place ou à distance, et un espace suffisant pour la réalisation des interventions dans des conditions normales.

Au cas où SNS SECURITY ne pourrait avoir accès aux locaux ou accomplir normalement l'installation et/ou la configuration du fait du Client, SNS SECURITY se réserve le droit de facturer le déplacement et le temps passé sur le site ou à distance même dans le cas où aucune installation et/ou configuration n'ont pu être réalisées.

D'une manière générale le Client devra fournir toute l'assistance nécessaire pour faciliter l'intervention de SNS SECURITY, de ses salariés et sous-traitants.

11 EQUIPEMENTS EN LOCATION OU PRETES

11.1 Equipements SNS SECURITY en Location ou prêtés

L'Equipement SNS SECURITY en Location ou prêté au Client est utilisé sous la seule responsabilité du Client et devra être restitué en bon état en fin de Contrat. Toute remise en état rendue nécessaire par une utilisation non-conforme, ou par une dégradation non-imputable à l'usage normal, sera à la charge du Client. Tout remplacement de l'Equipement SNS SECURITY sera à la charge du Client et devra être effectué par un personnel agréé par SNS SECURITY et après autorisation préalable écrite de celle-ci.

Le Client ou tout autre détenteur, s'interdit toute sous-location, concession d'usage, vente, prêt ou autre, sous quelque forme que ce soit, sous peine de résiliation du Contrat si bon semble à SNS SECURITY et sans préjudice de tous dommages et intérêts.

En cas d'éventuelles prétentions d'un tiers sur des Equipements SNS SECURITY, le Client s'engage à s'y opposer et à en avvertir immédiatement

SNS SECURITY ainsi qu'à faire le nécessaire pour que lesdits Equipements puissent être récupérés par SNS SECURITY ou à les lui restituer à sa demande.

De même, en cas d'ouverture d'une procédure collective à l'encontre du Client, ce dernier est tenu d'en aviser immédiatement SNS SECURITY et de rappeler par écrit à tout tiers le fait que SNS SECURITY demeure propriétaire des Equipements objets de la Location ou du prêt.

Pendant toute la durée du Contrat, le Client s'engage, à assumer les risques que pourraient subir les Equipements SNS SECURITY installés dans les locaux du Client ou de ses prestataires et à souscrire auprès d'une compagnie d'assurance notoirement solvable une assurance couvrant à hauteur de la valeur à neuf des Equipements SNS SECURITY confiés.

En cas de panne et/ou de sinistre d'un Equipement SNS SECURITY, le Client devra en informer sans délai SNS SECURITY par écrit sans préjudice de la déclaration à faire à la compagnie d'assurance dans les délais prévus.

En toutes circonstances, le Client devra obtenir l'accord de SNS SECURITY avant d'intervenir ou de faire intervenir un tiers sur l'Equipement SNS SECURITY.

Par ailleurs, le Client s'engage à ce que SNS SECURITY soit subrogée dans les droits du Client à l'indemnité versée par la compagnie d'assurance.

11.2 Restitution des Equipements SNS SECURITY en Location ou prêts

Au terme de la Location ou du prêt, il appartiendra au Client de restituer les Equipements SNS SECURITY ainsi que les consommables, objets du Contrat, non utilisés.

Dans le cas où les Equipements SNS SECURITY sont installés sur le site du Client ou dans un site d'hébergement tiers, et en cas de cessation du Contrat, le Client s'engage à démonter ou à faire démonter, sous sa responsabilité exclusive et à ses frais, les Equipements SNS SECURITY. Ces Equipements doivent être restitués par le Client, à l'adresse indiquée sur le Bon de Commande, dans des conditions garantissant la préservation de l'intégrité des Equipements SNS SECURITY. Le démontage et le retour des Equipements sont effectués, aux frais du Client et dans un délai de 15 jours ouvrés à compter de la date de cessation du Contrat, de la Location ou du prêt concerné.

SECURITY pourra à la demande du Client, établir un devis afin d'effectuer sous sa responsabilité, la reprise de l'Equipement.

Dans le cas où les Equipements SNS SECURITY seraient détériorés lors de leur démontage ou de leur restitution, ou en cas de non-restitution par le Client dans le délai de 15 jours précité, SNS SECURITY se réserve le droit de demander au Client le remboursement de l'Equipement SNS SECURITY détérioré ou non restitué sur la base du prix catalogue en vigueur au moment du constat de la détérioration ou de la non-restitution auquel il appliquera une remise de 30% (pour un Contrat de Location d'un an) ou 50% (pour un Contrat de Location de 3 ans). En outre, le Client devra verser à SNS SECURITY, à titre d'indemnité de jouissance, la somme de 15 € HT par jour de conservation de l'Equipement SNS SECURITY.

Le paiement de cette indemnité ne confère au Client aucun droit de conserver l'Equipement SNS SECURITY.

Il est enfin précisé qu'en cas de cessation de la Location, l'ensemble des licences de Logiciels intégrés au Matériel ainsi que les Services qui y sont rattachés cesseront de plein droit.

12 STRATEGIE ET SECURISATION MINIMALES DES SYSTEMES D'INFORMATIONS

Le Client reconnaît que la Cybersécurité est une préoccupation en constante évolution et qu'une protection absolue contre toutes les menaces et attaques ne peut être garantie.

Ainsi, le Client s'engage à fournir à SNS SECURITY toutes les informations nécessaires à la fourniture des services de Cybersécurité, y compris les détails sur les Equipements Client, systèmes informatiques, applications et données concernées par le Bon de Commande.

Le Client doit, au-delà des Services fournis par SNS SECURITY, veiller à définir et mettre en œuvre une politique de sécurité interne afin de prévenir toute intrusion ou utilisation frauduleuse de son système d'information.

Ainsi, le Client doit notamment mettre en place une solution de sécurisation de son réseau et de ses Equipements Client, mise régulièrement à jour, composée au minimum d'un pare feu ou de toute autre système préconisé par SNS SECURITY et a minima :

- Une évaluation des risques afin d'identifier les vulnérabilités et les menaces potentielles auxquelles les systèmes d'informations sont

exposés, l'objectif étant d'identifier les priorités en matière de sécurité et d'orienter les efforts de sécurisation.

- La définition et la mise en place d'une politique de sécurité claire, telle que des politiques d'accès aux données, de mots de passe, de sauvegarde, de gestion des incidents, etc. Ces politiques devront énoncer les règles et les bonnes pratiques à suivre par les utilisateurs des systèmes d'informations du Client.
- La mise en place des mécanismes de contrôle d'accès afin de restreindre l'accès aux systèmes d'informations et aux données sensibles uniquement aux utilisateurs autorisés. Cela peut inclure l'utilisation de mots de passe forts, d'authentification à deux facteurs, de restrictions d'accès basées sur les rôles, etc.

Le Client doit notamment interdire aux personnes non autorisées l'accès physique aux Equipements et conserver en lieu sûr et non accessible aux tiers les informations confidentielles liées aux Equipements installés (paramétrage, configuration, identifiants, mots de passe...) et ne les communiquer qu'aux seules personnes autorisées.

Le Client doit aussi veiller à ne jamais communiquer les mots de passe (à des partenaires, tiers, salariés non agréés...) et veiller à verrouiller au besoin le poste en dehors des périodes d'utilisation (vacances, pauses, absences...).

- Le Client devra s'assurer que les Logiciels, les systèmes d'exploitation et les applications utilisés dans les systèmes d'informations sont régulièrement mis à jour avec les derniers correctifs de sécurité afin de combler les vulnérabilités connues et réduire les risques d'exploitation par des pirates informatiques.
- Le Client devra former les utilisateurs des systèmes d'informations aux pratiques de sécurité de base, tels que la gestion des mots de passe, la détection des emails d'hameçonnage, la protection des données sensibles, etc. La sensibilisation à la sécurité est un prérequis pour impliquer les utilisateurs dans la protection des systèmes d'informations.
- Le Client met en place des mécanismes de surveillance des activités des systèmes d'informations pour détecter les comportements anormaux, les tentatives d'intrusion ou les activités suspectes par l'intermédiaire notamment de l'utilisation de journaux d'activité, de systèmes de détection d'intrusion, de surveillance du réseau, etc.
- Le Client met en place des politiques de sauvegarde régulières pour protéger les données contre la perte ou la corruption. Les sauvegardes doivent être réalisées de manière périodique et vérifiées pour s'assurer de leur intégrité.
- Le Client établit des procédures de gestion des incidents afin de gérer et répondre efficacement aux incidents de sécurité lorsqu'ils se produisent. Ces procédures peuvent inclure des plans de réponse aux incidents, des équipes d'intervention d'urgence et des canaux de communication clairs.

Le Client conséquemment reconnaît avoir été informé de ces préconisations considérées comme étant une information préalable.

13 UTILISATION DES SERVICES ET DES EQUIPEMENTS PAR LE CLIENT

Le Client utilise les Services et Equipements pour son usage strictement professionnel et exclusif et s'interdit de les mettre à disposition de tiers sous quelque forme que ce soit, sauf accord préalable et écrit de SNS SECURITY.

Le Client s'engage à mettre en œuvre les mesures de sécurité adéquates afin, notamment, d'empêcher d'éventuels branchements clandestins ou utilisation frauduleuse des Services et Equipements et garantit SNS SECURITY contre toutes les conséquences financières éventuelles de tels comportements.

Le Client est le seul responsable de l'utilisation des Services et Equipements et donc des conséquences de toute utilisation illégale, abusive, frauduleuse ou illicite des Services, Equipements et de leur Contenu, ou de toute autre utilisation des Services ou Equipements appartenant à SNS SECURITY par le Client ou par toute autre personne ou entité ayant accédé aux Services ou Equipements via le Client.

Le Client s'engage à mettre en œuvre l'ensemble des mesures de sécurité prescrites par les Fournisseurs des Equipements et, le cas échéant, rappelées par SNS SECURITY au travers, par exemple, des documents qu'elle lui adresse. Il s'engage également, à ce que ses utilisateurs suivent les formations relatives aux conditions de mise en œuvre ou de protection des Equipements, recommandées par leurs Fournisseurs ou par SNS SECURITY.

Le Client garantit SNS SECURITY contre tout dommage (en ce compris les frais de procédure et d'avocats), contre toute réclamation, action, revendication, procédure exercée à son encontre et qui résulterait de l'utilisation des Services, des Equipements ou des Contenus.

Le Client est le seul responsable de la réalisation d'une copie de sauvegarde de tous ses Logiciels, Contenus et données et du stockage de ces copies dans le lieu de son choix.

14 GARANTIE LEGALE

Le Client est expressément informé que SNS SECURITY n'est pas le fabricant des Matériels ni l'éditeur des Logiciels fournis dans le cadre des présentes.

SNS SECURITY n'a aucune obligation de garantie à l'égard du Client s'agissant des Logiciels souscrits directement auprès du Fournisseur. Selon les conditions définies par le Fournisseur, le Client pourra bénéficier des mises à jour et du support technique propres au Fournisseur.

Les Matériels vendus par SNS SECURITY bénéficient de la garantie légale contre tout défaut ou vice caché qui affecterait les Matériels.

En cas de vice caché, le Client pourrait exercer les actions reconnues par la loi et les tribunaux à l'acheteur d'une chose affectée d'un vice caché.

Afin de mettre en œuvre la garantie, le Client doit préalablement prendre contact avec le Support Technique de SNS SECURITY. Le Client doit retourner les Matériels accompagnés de leur facture de vente.

La garantie ne s'applique pas au cas de vices apparents, de défauts et détériorations provoqués par l'usure naturelle, d'un accident extérieur ou lorsque le vice allégué a pour origine une fausse manœuvre, une négligence, une modification du Matériel non prévue ni spécifiée, une mauvaise utilisation, une réparation ou un test non appropriés réalisés par le Client.

A défaut de souscription à un Service de Support Technique, et en cas de difficulté, le Client devra se retourner vers le Fournisseur. Dans tous les cas, SNS SECURITY ne saurait être tenue responsable en cas de refus du Fournisseur d'appliquer sa garantie.

Dans l'hypothèse où le Fournisseur du Matériel concerné aurait cessé de commercialiser les pièces et/ou composants dudit Matériel, SNS SECURITY ne sera pas soumis à un quelconque délai concernant l'éventuelle réparation du Matériel ou l'obtention desdites pièces et composants. Le cas échéant, SNS SECURITY pourra proposer au Client un nouveau Matériel, devant faire l'objet d'un nouveau Bon de Commande.

15 OBLIGATIONS ET RESPONSABILITES DES PARTIES

15.1 Obligations incombant à SNS SECURITY

SNS SECURITY s'engage à mettre en œuvre les moyens nécessaires en vue de fournir un Service continu dans la limite de la disponibilité des réseaux et des infrastructures des opérateurs auxquels le Client fait appel, ainsi que des contraintes techniques inhérentes à leur fonctionnement.

SNS SECURITY conseillera le Client dans les limites de ses engagements étant rappelé que SNS SECURITY ne fournit pas de conseil juridique, ni de conseil ayant trait à la veille technologique ou à l'innovation.

SNS SECURITY s'engage à fournir au Client le Matériel commandé tel que spécifié dans le Bon de commande.

Il est expressément convenu que SNS SECURITY est soumis à une obligation de moyens pour l'exécution de ses obligations. Les Parties conviennent expressément que la responsabilité de SNS SECURITY ne pourra être engagée par le Client qu'en cas de faute prouvée.

Par cela, SNS SECURITY s'engage à apporter, pour la réalisation des Services, les soins et la diligence d'un professionnel qualifié et à réaliser lesdits Services dans le respect de la législation alors applicable.

Notamment, SNS SECURITY décline toute responsabilité concernant le préjudice direct ou indirect, matériel ou immatériel, susceptible de résulter de l'intrusion dans le système du Client, ainsi que de l'utilisation dudit système, par des tiers non autorisés, causées par l'inexistence, l'insuffisance ou défaut de respect des procédures de Cybersécurité et de contrôle de l'accès au système dont il préconise la mise en œuvre par le Client. Le présent alinéa répartit le risque entre les Parties. Les prix convenus reflètent cette répartition du risque et la limitation de réparation qui en résulte.

15.2 Obligations spécifiques à la réalisation de tests d'intrusion à la charge de SNS SECURITY

En réalisant un test d'intrusion sur le système informatique ou les applications du Client, SNS SECURITY s'engage à fournir ses meilleurs efforts et à agir de

manière professionnelle afin d'identifier les vulnérabilités et les failles de sécurité possibles. Il est essentiel de noter que les tests d'intrusion ont leurs limites, en ce qu'il est impossible de garantir une détection exhaustive de toutes les vulnérabilités potentielles ainsi que des conséquences sur les paramétrages du système informatique dépendant de l'administration du système du Client.

Ainsi, SNS SECURITY ne sera pas responsable des dommages directs, indirects, matériels ou immatériels, résultant de l'exécution du test de pénétration, y compris, mais sans s'y limiter, les lenteurs, les défaillances des Equipements Clients, la perte de données, la perte de profits, les interruptions d'activité ou les dommages matériels.

La limitation de responsabilité concernant les tests d'intrusion ne s'applique pas en cas de négligence grave, de faute intentionnelle, de violation délibérée des obligations contractuelles essentielles ou de dommages corporels résultant de l'acte de SNS SECURITY. Celle-ci survivra en tout état de cause à la résiliation ou à l'expiration du présent Contrat pour quelque raison que ce soit.

En contractant avec SNS SECURITY afin d'effectuer le test d'intrusion, le Client reconnaît avoir lu, compris et accepté cette clause de limitation de responsabilité, ainsi que les termes et conditions du Contrat dans son ensemble. Le Client reconnaît également que cette limitation de responsabilité est une partie intégrante de la négociation entre les Parties et reflète une répartition raisonnable des risques liés au test de pénétration.

SNS SECURITY ne pourra être tenue pour responsable des altérations de données clientes issues des actions jugées nécessaires par les consultants de SNS SECURITY et permettant de délivrer le Service de test d'intrusion.

15.3 Responsabilité de SNS SECURITY

La responsabilité de SNS SECURITY ne pourra être engagée, qu'à raison des dommages directs et prévisibles subis par le Client du fait de SNS SECURITY.

Il est expressément rappelé que SNS SECURITY n'étant pas le seul prestataire intervenant sur les Equipements Client, SNS SECURITY ne pourra en aucun cas être tenue responsable à quelque titre que ce soit, des conséquences dommageables des agissements, erreurs ou fautes d'exécution imputables aux prestataires tiers intervenant pour le compte du Client sur ses Equipements et plus généralement sur son système informatique.

Sont considérés comme dommages indirects notamment les pertes de données, de temps, de bénéfices, de chiffre d'affaires, de marges, pertes de commandes, de clients, de chances, d'exploitation, de revenus, d'actions commerciales ou encore l'atteinte à l'image de marque, les résultats escomptés et l'action de tiers.

La responsabilité de SNS SECURITY est, tous faits générateurs confondus et tout préjudice confondu, limitée aux sommes effectivement versées par le Client au titre de la vente, la Location ou des Services en cause des six (6) derniers mois précédant la survenance du dommage, et en tout état de cause dans la limite maximale de 10 000 euros.

Si la durée du Contrat était inférieure à 6 mois, le montant des dommages-intérêts ci-dessus ne pourraient être supérieur à la durée effective du Contrat.

Le Client, ainsi que ses assureurs, pour lesquels il se porte fort, renoncent à tous recours contre SNS SECURITY au-delà de ce montant. La responsabilité de SNS SECURITY ne peut être engagée dans les cas de suspension, dégradation du Service, ou de dommages, liés à un cas de force majeure, ou en cas de faute de la part du Client ou d'un tiers, ou encore en cas d'interruption du Service sur demande du Client ou en cas de dysfonctionnement d'un Equipement Client.

Par ailleurs, et conformément aux dispositions de l'article 2254 du code civil, aucune action judiciaire visant à engager la responsabilité civile de SNS SECURITY ne pourra être intentée plus d'une année suivant la date où le Client a connu ou aurait dû connaître les faits lui permettant de l'exercer.

La responsabilité de SNS SECURITY ne pourra en aucun cas être engagée si le Client n'a pas lui-même respecté l'intégralité de ses obligations, telles que prévues aux présentes Conditions Générales et/ou Conditions Particulières.

Le Client devra par ailleurs faire son possible pour prendre les mesures raisonnablement nécessaires à la non-aggravation de son préjudice.

15.4 Obligations incombant au Client

Le Client déclare qu'il dispose des compétences requises pour apprécier la proposition d'intervention de SNS SECURITY. Le Client déclare mettre en œuvre sous sa seule responsabilité les conseils de SNS SECURITY.

Le Client s'engage à respecter toutes les lois et réglementations applicables en matière de Cybersécurité et à ne pas utiliser les Services de Cybersécurité à des fins illicites ou malveillantes.

Le Client s'engage par ailleurs à informer sans délais SNS SECURITY de toute modification ou évolution des Equipements Client, ou des outils de connexion

à son système d'information, telles que les montées de versions ou l'installation de nouvelles applications compris dans le périmètre des Services.

Le Client s'interdit de faire intervenir un tiers sur les Services et Equipements objets du Contrat. A défaut, SNS SECURITY se réserve le droit de refuser d'intervenir et pourra, si elle le souhaite résilier le Contrat aux torts exclusifs du Client.

15.5 Obligations spécifiques à la souscription d'un Logiciel

La souscription à un Logiciel par le Client se fait en toute circonstance sous sa responsabilité. Ainsi, il doit se référer et respecter les conditions appliquées par le Fournisseur.

Par ailleurs, le Client utilisera les Logiciels conformément à leur destination et aux spécifications du Fournisseur et de SNS SECURITY et dans le respect de la réglementation applicable notamment en termes de protection des Données Personnelles.

15.6 Responsabilité du Client

Le Client garantit SNS SECURITY contre toutes les conséquences des réclamations, actions et revendications qui pourraient être intentées à l'encontre de SNS SECURITY par des tiers et se rapportant à des dommages causés à ces derniers soit par les Equipements Client soit par la suite d'une manipulation ou d'une intervention sur les Equipements, ou du fait d'une utilisation anormale des Equipements ou des Services, du fait de ses personnels, sous-traitants, partenaires ou plus généralement de son activité.

16 MODIFICATION/SUSPENSION DE LA FOURNITURE DU SERVICE

16.1 A l'initiative de SNS SECURITY

SNS SECURITY se réserve le droit de modifier à tout moment les caractéristiques du Service notamment en fonction des évolutions réglementaires ou des évolutions des normes et standards en vigueur.

SNS SECURITY peut suspendre la fourniture du Service en cas de risque pour le bon fonctionnement ou la sécurité de ses infrastructures ou des Equipements SNS SECURITY ou des équipements de tiers, en cas d'interventions techniques ou de maintenance de SNS SECURITY, en cas de fraude détectée ou rapportée, et en cas d'usage abusif, frauduleux, illicite suspecté ou rapporté du Service par le Client.

Sauf cas d'urgence, SNS SECURITY en informera préalablement le Client dans les plus brefs délais. SNS SECURITY ne peut être tenue responsable des conséquences d'une suspension ou de l'altération du Service liés aux circonstances décrites ci-dessus. La suspension ou l'altération du Service constatées dans ces conditions ne donnera pas davantage lieu à l'application de pénalités prévues par les présentes ou par les Conditions Particulières de Service ni, pour le Client, au droit de résoudre le Contrat.

16.2 A la demande du Client

Les modifications du Service demandées par le Client et acceptées par SNS SECURITY s'opèrent par voie d'avenant au Bon de Commande signé par les deux Parties.

17 GARANTIES DE QUALITE DE SERVICE – SUPPORT TECHNIQUE

17.1 Catégories de garanties

Selon les Services souscrits, SNS SECURITY peut s'engager à respecter des garanties de qualité de Service au profit du Client. Ces garanties de qualité de Service peuvent concerner :

- la garantie de délai d'intervention ;
- la garantie de délai de rétablissement ou délai de résolution;
- la garantie de taux de disponibilité ;
- toute autre garantie spécifique prévue dans les Conditions Particulières de Service.

Les niveaux d'engagement des garanties de Service sont définis dans les Conditions Particulières de Service.

La qualité du Service attendue est déterminée dans le Bon de Commande ou le cas échéant dans les Conditions Spécifiques ou un plan d'assurance qualité remis au Client par SNS SECURITY.

Le Client est informé que SNS SECURITY n'est pas responsable de la qualité, de la disponibilité et de la fiabilité des réseaux de télécommunications, quelle que soit leur nature, en cas de transport de données ou d'accès Internet.

En outre, les Fournisseurs des Equipements peuvent s'engager sur des niveaux de services propres à leurs Equipements. En cas de modification desdits niveaux de services par les Fournisseurs au cours du Contrat, SNS SECURITY s'engage à en informer le Client dans les meilleurs délais par tout moyen écrit à sa convenance. En cas de désaccord, le Client doit obligatoirement en aviser SNS SECURITY par lettre recommandée avec accusé de réception dans un délai de 15 jours calendaires suivant la date de cette notification, faute de quoi, il sera réputé avoir accepté les nouveaux niveaux de services.

En cas de refus des nouveaux niveaux de services du Fournisseur, le Client pourra résilier la souscription au Service ou la Location de l'Equipement concerné par cette modification, selon les modalités de l'article « Résiliation » des présentes.

17.2 Gestion des Incidents

17.2.1 Notification d'un Incident

Le Client peut contacter le Support Technique afin de signaler des Incidents aux jours et heures indiqués dans l'extranet Client, ou à défaut aux Heures et Jours Ouvrés. Si le Client souscrit au service d'astreinte, il pourra contacter le support technique 24h/24, 7j/7j aux contacts qui lui seront communiqués.

Cette notification peut être réalisée par téléphone, télécopie, courrier électronique ou via l'extranet Client.

17.2.2 Ticket d'Incident

Chaque Incident notifié au Support Technique fait l'objet de l'attribution, par SNS SECURITY, d'un numéro de ticket d'Incident.

Le ticket d'Incident est fermé par SNS SECURITY quand le Service est rétabli. Le ticket d'Incident mentionne le moment où il a été ouvert, celui où le Service a été rétabli ainsi que la durée totale de l'Incident.

Si l'Incident résulte d'un élément ou d'un Equipement Client non vendu ou fourni par SNS SECURITY, l'intervention du Support Technique est facturée au tarif en vigueur.

17.2.3 Période d'intervention du Support Technique

Le Support Technique de SNS SECURITY intervient uniquement les Jours et Heures Ouvrés.

En option, le Client peut demander que l'intervention du Support Technique soit étendue 24 heures /24 et 7 jours /7.

17.2.4 Délai d'intervention

Le délai d'intervention du Support Technique s'entend du délai entre l'attribution du numéro de ticket d'Incident et la communication au Client d'un premier diagnostic comprenant notamment l'origine supposée de l'Incident et un délai estimatif de résolution de l'Incident.

Le délai d'intervention est automatiquement suspendu en dehors des Heures et Jours Ouvrés sauf mention contraire dans les Conditions Particulières.

Toute période pendant laquelle le Client ne peut assister SNS SECURITY dans les opérations de diagnostic, notamment pour fournir des informations nécessaires à ces opérations, réaliser des tests ou accéder aux Equipements et/ou site du Client, n'est pas prise en compte dans le calcul du délai d'intervention.

17.2.5 Délai de rétablissement ou délai de résolution

Le délai de rétablissement ou délai de résolution s'entend du délai entre le numéro d'attribution du ticket d'Incident et la résolution de l'Incident telle qu'indiquée sur le ticket d'Incident. La résolution des Incidents pourra consister notamment au choix de SNS SECURITY en un paramétrage ou encore une solution de contournement.

Le délai d'intervention est automatiquement suspendu en dehors des Heures et Jours Ouvrés sauf souscription du service d'astreinte. Toute période pendant laquelle le Client ne peut assister SNS SECURITY dans la résolution de l'Incident, notamment pour fournir des informations nécessaires à la résolution de l'Incident, réaliser des tests ou accéder aux Equipements et/ou site du Client, ne sera pas prise en compte dans le calcul du délai de rétablissement ou délai de résolution.

17.2.6 Taux de disponibilité

Le taux de disponibilité s'entend d'un taux de continuité de fourniture du Service calculé en minutes sur une période de 12 mois glissants. Ce taux est précisé dans les Conditions Particulières du Service concerné.

18 PROPRIETE INTELLECTUELLE

SNS SECURITY est titulaire exclusif des droits de propriété intellectuelle relatifs au Service ou bénéficie des droits lui permettant de conclure le Contrat.

Le Client s'interdit de reproduire, représenter, utiliser, adapter, modifier, reconstituer, traduire, commercialiser ou obtenir un accès non-autorisé aux Logiciels, outils, Matériels, contenus, design, conception, architecture, données et documentations utilisées par SNS SECURITY dans le cadre des Services, sans que cette liste ne soit exhaustive.

Toute reproduction ou représentation, totale ou partielle d'un de ces éléments par le Client, sans l'autorisation expresse de SNS SECURITY est interdite et constituerait une contrefaçon de la part du Client.

SNS SECURITY conserve la propriété de ses méthodes et son savoir-faire sur les Services.

Le Contrat ne constitue en aucun cas une licence ou un transfert de propriété sur les droits détenus par SNS SECURITY à l'égard du Client.

Lorsque que le Client souscrit auprès de SNS SECURITY des Services portant sur des Equipements Clients non fournis ou vendus par SNS SECURITY, il garantit disposer de tous les droits et autorisations nécessaires à leur réalisation. A ce titre, le Client garantit SNS SECURITY contre toute action, réclamation, revendication ou opposition de la part de toute personne invoquant un droit, de propriété intellectuelle ou autre, un acte de concurrence déloyale et/ou parasitaire, auquel l'exécution du présent Contrat aurait porté atteinte.

19 ASSURANCE

Les Parties déclarent être assurées pour toutes les conséquences dommageables et les actes dont elles pourraient être tenues responsables dans le cadre des présentes auprès d'une compagnie d'assurance notoirement solvable et établie en France.

20 PERSONNEL – SOUS-TRAITANCE

SNS SECURITY s'engage à ce que son personnel, lors de l'intervention sur le site du Client ou les Equipements Client, prenne connaissance et applique les règles et consignes qui lui seront communiquées.

SNS SECURITY s'interdit de recourir au travail dissimulé, conformément aux articles L. 8221-1 et L. 8221-5 du Code du travail, et plus généralement s'engage à respecter l'ensemble de ses obligations définies dans le même code.

Le Client s'engage à ne pas débaucher ou embaucher, directement ou indirectement, le personnel de SNS SECURITY pendant toute la durée du Contrat et pendant une durée de trente-six mois (36) à compter de la cessation des relations contractuelles. En cas de non-respect par le Client des obligations prévues dans la présente clause, celui-ci s'engage à verser à SNS SECURITY une pénalité égale à trente-six mois du dernier salaire brut mensuel de la ou des personnes en cause.

Le Client autorise SNS SECURITY à faire intervenir tout sous-traitant de son choix. Dans ce cas, le Client accepte que SNS SECURITY divulgue auxdits sous-traitants les informations nécessaires à l'exécution des présentes. SNS SECURITY s'engage à garantir le respect des obligations de confidentialité prévues aux présentes auprès du sous-traitant choisi.

SNS SECURITY se réserve la possibilité d'utiliser tout sous-traitant qu'il jugera utile, dès lors que ce dernier présente toutes les qualités requises de professionnalisme et de pérennité. SNS SECURITY se portera en tout état de cause garant vis-à-vis du Client de l'ensemble des Services et obligations à sa charge visées dans les présentes et en informera le Client.

21 CONDITIONS FINANCIERES

21.1 Prix du Service

Les prix hors taxes sont indiqués en euros et sont définis dans le Bon de Commande.

Les droits et taxes, supportés par le Client, sont ceux applicables au jour de la facturation en application de la législation française.

21.2 Révision du prix

SNS SECURITY peut modifier ses tarifs et appliquer les nouveaux tarifs aux Contrats en cours d'exécution selon les dispositions ci-après.

Le tarif est révisable une fois par an sauf information contraire dans le Bon de Commande, généralement au 1er janvier de chaque année, sur la base du dernier indice SYNTEC publié par l'INSEE selon la formule : $P1 = P0 \times (S1 / S0)$

P1 : prix révisé

P0 : prix contractuel d'origine

S0 : indice SYNTEC de référence retenue à la date de conclusion du Contrat

S1 : dernier indice publié à la date de révision

Dans ce cas, SNS SECURITY informe au préalable par écrit les Clients concernés deux mois au plus tard avant la date de prise d'effet de cette révision. En cas d'augmentation au-delà de 10% d'un ou de plusieurs tarifs, le Client peut résoudre, librement et sans pénalité, le Service souscrit qui a fait l'objet de l'augmentation après avoir notifié cette résolution par lettre recommandée avec accusé de réception à SNS SECURITY dans un délai de 15 jours à compter de la réception de la lettre de SNS SECURITY l'informant de cette augmentation.

21.3 Facturation

Les factures sont établies selon les termes prévus au Bon de commande à savoir mensuellement, trimestriellement ou annuellement.

Les redevances mensuelles, trimestrielles ou annuelles forfaitaires des Services sont facturées terme à échoir à compter de leur Date de Mise à disposition telle que définie à l'article 5 des présentes.

Les Consommations éventuelles sont facturées à terme échu ou à échoir si ces consommations peuvent faire l'objet d'une estimation fiable. En tout état de cause, une régularisation à terme échu des Consommations sera établie en cas d'écart avec les estimations.

SNS SECURITY pourra à tout moment choisir d'émettre ses factures sous forme électronique conformément à l'article 289-VII 1° du code général des Impôts. Le Client s'engage ainsi à fournir sur simple demande toutes les informations nécessaires à la mise en œuvre de ce mode de transmission et accepte de recevoir les factures au format électronique.

En cas de difficultés, telles qu'évoquées à l'article 10 des présentes, SNS SECURITY facture les frais d'installation ou de mise en service de chaque Service à la Date de Mise à disposition ou à la date de réunion de lancement de projet.

En cas de vente d'un Equipement par SNS SECURITY au Client, SNS SECURITY facture le prix de l'Equipement à la date de livraison au Client.

En cas de Location d'un Equipement SNS SECURITY, cette dernière facture les loyers en terme à échoir à compter de la Date de Mise à disposition effective de l'Equipement SNS SECURITY. Le prix de la Location est payable par prélèvement selon la périodicité indiquée sur le Bon de commande. Il est expressément précisé au Client que la facturation liée à la Location de Logiciel démarrera à compter de sa mise à disposition au Client et ce nonobstant l'absence d'activation ou l'activation postérieure des licences de Logiciels par le Client.

Pendant les douze (12) mois qui suivent la date de paiement de la facture, SNS SECURITY tient à la disposition du Client les éléments d'information suffisants pour justifier des factures. Au-delà de ce délai, aucune facture ne peut faire l'objet d'une contestation de la part du Client.

Les contestations de factures devront reposer sur des preuves documentées et communiquées dans un bref délai à compter de la réception des factures.

En cas de contestation ne portant que sur une partie des factures, la partie non contestée devra être réglée par le Client dans le délai contractuel visé dans les présentes.

21.4 Modalités de paiement

Les factures réglées par prélèvement bancaire automatique sont payables à date d'établissement de la facture sauf précision contraire dans le Bon de Commande.

Les factures soumises aux autres modes de règlement (virement bancaire, chèque et mandat administratif) sont payables à trente (30) jours nets à compter de la date d'établissement de la facture.

Aucun escompte n'est consenti par SNS SECURITY en cas de paiement anticipé. La défaillance de paiement par le Client entraîne l'exigibilité immédiate du paiement correspondant par le Client.

Un acompte dont le montant sera déterminé sur le Bon de Commande pourra être exigé lors de la passation de la commande par le Client.

Dans le cadre de la reconduction de la souscription des Services, le paiement du prix des Services devra intervenir en totalité, au plus tard à la date anniversaire de la souscription.

SNS SECURITY se réserve le droit d'exiger du Client au moment de la signature du Bon de Commande et/ou à tout moment de la durée du Contrat, un dépôt de garantie restitué dans les 30 jours de la cessation du Contrat sous réserve de l'imputation sur ce montant d'éventuelles pénalités de retard de

paiement ou du prix des Equipements SNS SECURITY non-restitués ou détériorés à l'expiration du Service ou de la Location.

21.5 Défaut de paiement

En cas de non-paiement à l'échéance d'une facture, SNS SECURITY peut, de plein droit après mise en demeure :

- suspendre après un préavis de 15 jours l'exécution du Contrat ;
- prononcer, de plein droit, la résolution du Contrat sans préjudice de tous autres dommages et intérêts que SNS SECURITY serait en droit de réclamer.

Le retard de paiement entraîne également la déchéance de tous les termes des créances de SNS SECURITY sur le Client et leur exigibilité immédiate, sans préjudice de toute autre action que SNS SECURITY serait en droit d'intenter, à ce titre, à l'encontre du Client.

Le retard de paiement donne lieu à l'application d'un intérêt de retard égal à 4 fois le taux d'intérêt légal, et à la facturation d'une indemnité forfaitaire pour les frais de recouvrement d'un montant de 40 Euros, sans formalité aucune ni mise en demeure préalable, sans préjudice de toute autre action que SNS SECURITY serait en droit d'intenter, à ce titre, à l'encontre du Client. SNS SECURITY se réserve le droit de demander au Client une indemnisation complémentaire si les frais de recouvrement effectivement engagés dépassaient ce montant, sur présentation des justificatifs.

En cas de modification de la situation du Client, ou d'incident ou retard de paiement, SNS SECURITY aura également la faculté de modifier les délais de règlement accordés ou d'exiger des garanties, y compris au titre des Services en cours.

Enfin, SNS SECURITY se réserve le droit d'exiger le règlement de toute somme due ou dettes contractées vis-à-vis de SNS SECURITY avant la passation d'un nouveau Bon de Commande.

22 RESILIATION

22.1 Résiliation du Contrat

Sauf stipulations contraires et sous réserve qu'aucun Service ne soit en Période Minimale d'engagement, chacune des Parties peut, sans indemnité, notifier à l'autre Partie la résiliation du Contrat à son terme moyennant un préavis de trois (3) mois avant la date d'anniversaire du Contrat, sous réserve de préavis plus long spécifiques à certains Services.

Dans le cas où la résiliation du Contrat est effectuée alors qu'un Service est toujours en Période Minimale d'engagement, la résiliation se fait moyennant le versement d'une indemnité égale à la totalité des redevances restant dues jusqu'à l'expiration de la Période Minimale, sans omettre les frais de mise en service, d'installation et d'achat d'Equipements restant le cas échéant dus à SNS SECURITY.

La résiliation de l'ensemble des Services entraînera la résiliation du Contrat dans son intégralité.

22.2 Résiliation d'un Service

22.2.1 Résiliation pour convenance

La résiliation d'un Service peut être prononcée, pour convenance, moyennant l'application d'un préavis de trois (3) mois avant la date d'anniversaire du Service pour les liens d'accès internet et/ou mobile opérateur ou d'un préavis de trois (3) mois avant la date d'anniversaire du Service pour les autres Services à compter de l'envoi d'une lettre recommandée avec avis de réception. Cette résiliation peut donner lieu au versement d'une indemnité égale à la totalité des redevances ou abonnements restant dus jusqu'à l'expiration de la Période Minimale, sans omettre les frais de mise en service, d'installation et d'achat d'Equipements restant le cas échéant dus à SNS SECURITY.

22.2.2 Résiliation d'un contrat indispensable au Service

Le Service peut également être résilié par SNS SECURITY, à tout moment, dans le cas où un des contrats nécessaires à la fourniture de ce Service, conclu par SNS SECURITY avec un tiers, est résilié. La résiliation du Service considéré est prononcée moyennant l'envoi, par SNS SECURITY au Client, d'une lettre recommandée avec accusé de réception appliquant un préavis d'au moins 15 jours. Cette résiliation ne donne droit à aucune indemnité de part et d'autre.

22.2.3 Résiliation et devis complémentaire

Le Service peut également être résilié par SNS SECURITY en cas de non-acceptation par le Client d'un devis complémentaire afin de mettre à niveau les Equipements du Client nécessaire à l'exécution du Service dans les règles de l'art. Cette résiliation sera prononcée de plein droit en cas de refus notifié par le Client à SNS SECURITY ou en l'absence d'acceptation dans un délai de 15

Jours Ouvrés à compter de la date d'établissement du devis complémentaire. Cette résiliation n'entraîne le paiement d'aucune indemnité ou pénalité de part et d'autre.

22.3 Résiliation pour faute

En cas de manquement de l'une des Parties dans l'exécution d'une obligation essentielle prévue au Contrat, l'autre Partie peut résilier de plein droit le Contrat s'il n'est pas remédié à ce manquement dans un délai de trente (30) jours, après une mise en demeure adressée par l'autre Partie par lettre recommandée avec avis de réception. Pour l'application du présent article, sont considérées comme des obligations essentielles des Parties, les obligations qui leur sont propres stipulées aux clauses suivantes :

- Pour le Client : articles 8, 10, 11, 12, 13, 15, 18, 21, 25, 26 et 28.1 ;
- Pour SNS SECURITY : articles 14, 15, 17, 19, 20 et 26.

Cette résiliation est prononcée sans préjudice du droit de l'une ou de l'autre des Parties à obtenir l'indemnisation de son préjudice causé par un manquement non réparé de l'autre Partie ni du droit de SNS SECURITY à réclamer le paiement de l'éventuel montant minimum annuel de facturation/Consommation, ainsi que le montant des redevances ou abonnements dans les cas où cette résiliation interviendrait, à sa demande, et alors qu'un Service serait encore affecté d'une Période Minimale d'engagement.

23 CONSEQUENCES DE LA CESSATION DU CONTRAT

Au terme du Contrat, pour quelque cause que ce soit les Services souscrits par le Client cesseront.

Toutes les sommes dues par le Client deviendront immédiatement exigibles. De surcroît, SNS SECURITY se réserve le droit de facturer les montants restants dus jusqu'au terme des Services en cours à la date de résiliation si cette dernière est imputable au Client ou si elle intervient avant le terme de la Période Minimale d'engagement.

Le Matériel SNS SECURITY qui aurait été mis à disposition du Client dans le cadre des Services ou d'une Location devra être restitué à SNS SECURITY conformément aux stipulations des présentes quant à leur état.

La restitution du Matériel sera faite par le Client à ses frais et sous sa responsabilité au siège social de SNS SECURITY.

En cas de cessation des Services pour quelque cause que ce soit, le Client, s'il souhaite poursuivre l'utilisation d'un Logiciel, devra faire son affaire personnelle de la poursuite du contrat de licence dudit Logiciel directement auprès du Fournisseur.

24 PROTECTION DES DONNEES PERSONNELLES

Le Client est seul responsable des Données Personnelles qu'il détient et fera tout son possible pour ne pas communiquer ces données à SNS SECURITY et/ou à les anonymiser avant toute communication. Dans le cas cependant où SNS SECURITY serait amenée, dans le cadre de la réalisation des Services, à avoir accès à de telles données, il est entendu entre les Parties qu'elle agira en tant que sous-traitant du Client et s'engage à ce titre à prendre toutes les mesures nécessaires pour conserver ces données confidentielles et à les traiter conformément aux instructions du Client. Le cas échéant, la sous-traitance de ces Données Personnelles est réalisée par SNS SECURITY dans les conditions prévues au sein de l'accord de sous-traitance conclu entre les Parties et annexé au présent Contrat.

25 EXTRANET

Dans l'éventualité de la mise en place par SNS SECURITY d'un extranet, extension de son système d'information permettant au Client d'avoir accès à des informations, un accès via internet par une connexion sécurisée sera mis à disposition du Client avec un accès par mot de passe.

Les mots de passe sont strictement personnels et confidentiels. Le Client s'assurera des conditions de sécurité desdits accès.

Aucune opération ne peut être effectuée par un Client sans ses codes d'accès.

Le Client s'engage à ne pas divulguer à autrui son mot de passe et est seul responsable de la confidentialité de son mot de passe et de sa préservation et, donc, des conséquences d'une divulgation involontaire à quiconque.

Toute utilisation de l'extranet à partir du mot de passe attribué au Client est présumée comme émanant exclusivement du Client.

Le Client est responsable, selon le droit commun, des actes et agissements de toute personne utilisant son compte, même à son insu, et donc de la préservation de la confidentialité de son identifiant, de son mot de passe et/ou de toute information personnelle qu'il a transmise à SNS SECURITY.

Le Client s'engage à signaler à SNS SECURITY dans les plus brefs délais toute utilisation frauduleuse de son compte, de son pseudonyme ou de son mot de passe dont il aurait connaissance.

26 CONFIDENTIALITE

Pendant toute la durée du Contrat et pendant une durée de cinq (5) ans à compter de son expiration ou de sa résolution, les Parties s'engagent à garder strictement confidentielles toutes les informations qu'elles auront été amenées à recueillir à l'occasion de leurs relations contractuelles par écrit ou oralement, y compris les informations communiquées ou obtenues à l'occasion des négociations relatives au Contrat. Les Parties doivent prendre les mesures raisonnablement nécessaires pour empêcher toute divulgation ou utilisation non autorisée de telles informations par leurs employés ou par des tiers. Les Parties s'engagent à utiliser les informations confidentielles de l'autre Partie aux fins exclusives d'exécution de ses obligations définies au Contrat. Elles s'interdisent de publier, communiquer, divulguer, mentionner, oralement ou par écrit, en tout ou partie, et à quelque tiers que ce soit, les informations confidentielles de l'autre Partie. Il est toutefois précisé que chacune des Parties pourra transmettre les informations confidentielles à ses collaborateurs et à des tiers, dès lors que cela est nécessaire à l'exécution du Contrat et que ces derniers sont soumis à une obligation de confidentialité.

L'engagement de confidentialité figurant dans les présentes ne s'appliquera pas aux informations dont la Partie récipiendaire peut apporter la preuve :

- qu'elles étaient dans le domaine public au moment de leur communication par l'autre Partie ou viendraient à tomber dans le domaine public postérieurement à cette communication sans que cela résulte dans ce dernier cas d'une violation d'une obligation de confidentialité souscrite par la Partie recevant les informations ou ;
- qu'elles étaient déjà connues licitement par la Partie récipiendaire avant leur première communication à celle-ci ou ;
- que la Partie récipiendaire les a reçues d'un tiers de bonne foi n'ayant lui-même vis-à-vis de l'autre Partie aucune obligation de confidentialité concernant ces informations ou ;
- que les informations ont été divulguées à la demande d'une autorité administrative ou conformément à l'application de dispositions législatives ou réglementaires ou suite à une transaction ayant reçu un caractère exécutoire ou une décision de justice.

Toutes les informations confidentielles communiquées par une Partie demeurent sa propriété exclusive, tout transfert de droits sur lesdites informations au bénéfice de la Partie réceptrice étant exclu.

Chaque Partie se porte fort à l'égard de l'autre du respect par tout membre de son personnel ou tout prestataire intervenant pour son compte du respect de la confidentialité des informations confidentielles.

27 FORCE MAJEURE

La force majeure s'entend de tout événement échappant au contrôle des Parties et qui ne pouvait être raisonnablement prévu lors de la conclusion du Contrat au sens de l'article 1218 du Code Civil et de son interprétation par la jurisprudence française, et qui a pour effet d'empêcher l'exécution des obligations de l'une ou l'autre des Parties.

Les Parties s'accordent sur le fait que sont notamment assimilés à des cas de force majeure les grèves internes ou externes, notamment chez un Fournisseur délivrant des services liés directement ou indirectement à la Cybersécurité en France ou à l'étranger, les lock out, les incendies, inondations, les dégâts des eaux, ou autres catastrophes naturelles, les épidémies, les pandémies touchant plus de 10% du personnel d'une Partie, les blocages de routes et les impossibilités d'approvisionnement de fournitures, les attentats, les guerres, les opérations militaires ou les troubles civils, les blocages des moyens de transport ou d'approvisionnement, l'absence de fourniture d'énergie, l'arrêt partiel ou total du réseau Internet et, de manière plus générale, des réseaux de télécommunications privés ou publics, la défaillance d'un tiers, y compris un Fournisseur, ainsi que la modification de toute réglementation applicable au Contrat et en rendant l'exécution impossible ou déraisonnablement onéreuse, une coupure d'alimentation électrique sur le site Client ou une coupure d'alimentation électrique de plus de vingt-quatre (24) heures sur un site de SNS

SECURITY, et tout autre cas indépendant de la volonté expresse de SNS SECURITY empêchant l'exécution normale des présentes.

Chaque Partie notifiera, dans les meilleurs délais, à l'autre Partie par lettre recommandée avec avis de réception la survenance de tout cas de force majeure.

Dans un premier temps, la force majeure suspend l'exécution des obligations de la Partie qui s'en prévaut. L'exécution du Contrat est prorogée d'une durée égale à la durée des événements constitutifs de la force majeure et reprend dès la date de cessation de l'évènement de force majeure.

Si, après un délai de quinze (15) jours à compter du début de l'évènement de force majeure, les conséquences du cas de force majeure persistent, les Parties doivent se réunir pour trouver une solution satisfaisante. A défaut d'accord dans un délai d'un mois, le Contrat pourra être résilié à l'initiative de la Partie la plus diligente.

28 STIPULATIONS FINALES

28.1 Intuitu personae

La relation entre les parties étant « intuitu personae » à l'égard du Client, il s'interdit, d'une part de transférer, pour quelque cause et sous quelque forme que ce soit, à titre onéreux ou gratuit, l'un quelconque de ses droits et obligations à un tiers et, d'autre part de confier à un tiers, l'exécution de tout ou partie de ses obligations contractuelles.

De surcroît, en cas de modifications qui pourraient intervenir dans la personne du Client, telles que par exemple, fusion, scission, absorption, apport partiel d'actif, cession, transfert à une filiale, cession de plus de 50% des titres par l'un ou plusieurs des associés, changement de dirigeant et tout autre accord juridique ou commercial avec un tiers, le Client doit informer SNS SECURITY 90 jours avant la réalisation de l'opération cette dernière se réservant le droit de résilier le Contrat en cas de non-respect de cette formalité et/ou en cas de réalisation de l'opération envisagée quand bien même elle en aurait été informée.

L'« intuitu personae » n'étant pas réciproque, la solvabilité du Client devant être vérifiée, les modifications qui pourraient intervenir dans la personne de SNS SECURITY, telles que par exemple, fusion, scission, absorption, apport partiel d'actif, cession, transfert à une filiale et tout autre accord juridique ou commercial avec un tiers, seraient sans effet sur l'existence ou l'exécution du Contrat. Le Client donne également son accord à ce que SNS SECURITY puisse librement transférer ou céder tout ou partie du Contrat à un tiers.

Cependant, ces interdictions ne pourront pas être opposées aux obligations légales d'ordre public ni à l'autorisation écrite et préalable des parties.

28.2 Intégralité du Contrat - Modification - Renonciation

Le Contrat, tel que défini à l'article 3, constitue l'intégralité de l'accord entre les Parties et prévaut sur toutes les discussions, négociations, propositions et conventions antérieures entre les Parties en ce qui concerne l'objet des présentes.

Le défaut de l'une des Parties de faire valoir ses droits au titre du Contrat ne sera pas réputé valoir renonciation à ce droit et aucune renonciation expresse à un droit ne sera réputée constituer une renonciation à un autre droit.

Aucune dérogation aux présentes Conditions Générales, et notamment les conditions générales d'achat du Client, ne sera opposable à SNS SECURITY à moins que celle-ci ne les ait acceptées préalablement à la conclusion du Contrat et par écrit.

Aucune modification du Contrat ne sera prise en compte par SNS SECURITY après sa conclusion sauf accord exprès de SNS SECURITY et ajustement éventuel du Bon de Commande y afférent.

28.3 Avis et notifications

Les avis et notifications prévus dans le Contrat sont adressés à leur destinataire par lettre recommandée avec accusé de réception ou par télécopie ou courrier électronique confirmé par lettre recommandée avec accusé de réception sauf lorsqu'il est expressément prévu un autre moyen. Chaque notification se fera aux adresses indiquées en bas des présentes à l'attention de la Direction pour ce qui concerne l'adresse de SNS SECURITY et dans le Bon de Commande pour ce qui concerne l'adresse du Client, le tout sous réserve d'un changement d'adresse pendant la durée du Contrat qui sera notifié à l'autre Partie conformément aux présentes.

28.4 Absence de relation entre les Parties

Aucune stipulation du présent Contrat ne sera réputée créer une relation de mandat, un partenariat, un contrat de société ou une co-entreprise (joint-

venture) entre les Parties ou leurs sociétés affiliées, employés, dirigeants ou administrateurs respectifs.

28.5 Autonomie des stipulations

Si une stipulation du Contrat est jugée illégale ou nulle par tout tribunal, autorité administrative, tribunal arbitral ou entité du gouvernement, toutes les autres stipulations du Contrat restent en vigueur et de plein effet. Les Parties s'engagent à collaborer de bonne foi pour remplacer la stipulation nulle ou illégale dès que possible par une nouvelle stipulation ayant un résultat licite aussi proche que possible du résultat que visait la stipulation frappée de nullité.

28.6 Titres

Les titres utilisés dans le Contrat ne sont donnés qu'à titre indicatif et ne sauraient en aucun cas affecter le sens des clauses contractuelles auxquelles ils se rapportent.

28.7 Mode de preuve

Le Client accepte que la facturation, les performances, la Consommation et plus généralement l'ensemble des mesures relatives à l'utilisation du Service, soient calculés avec les outils de SNS SECURITY et sur la base des données enregistrées par SNS SECURITY.

Les Parties conviennent que tout document ou correspondance sous forme électronique échangés entre les Parties, ainsi que les journaux, registres et logs de connexion informatiques, seront valablement considérés comme les preuves des communications intervenues entre les Parties, des Consommations et de l'utilisation des Services. Les Parties conviennent d'informer leurs collaborateurs de la validité de ces preuves de communications.

28.8 Référence commerciale - promotion

Le Client autorise SNS SECURITY à utiliser son nom à titre de référence commerciale. Si le Client a concédé un droit identique au profit d'un concurrent de SNS SECURITY, le Client demeure seul responsable des revendications de toute nature de ce concurrent qui pourraient naître du fait de cette utilisation.

Le Client autorise SNS SECURITY à lui adresser par tout procédé de télécommunication ou par courrier des informations périodiques, des publicités, ou offres commerciales, des invitations à caractère événementiel.

28.9 Litiges / Droit applicable

Le Contrat est régi par le droit français.

En cas de difficulté de toute nature et avant toute procédure juridictionnelle, les Parties tenteront de trouver une solution amiable conciliant leurs intérêts mutuels dans le respect du Contrat.

EN CAS DE LITIGE, COMPETENCE EXPRESSE EST ATTRIBUEE AU TRIBUNAL DE COMMERCE DE MONTPELLIER, NONOBTANT LA PLURALITE DE DEFENDEURS OU L'APPEL EN GARANTIE MEME POUR LES PROCEDURES D'URGENCE OU POUR LES PROCEDURES CONSERVATOIRES, EN REFERE OU PAR REQUETE.

IL EST PREALABLEMENT EXPOSE ET DECLARE CE QUI SUIIT :

Le Responsable de Traitement est client de la société Sous-Traitante. Il a souhaité souscrire aux services définis dans le Contrat proposés par le Sous-Traitant à ses clients. Afin de fournir ces prestations, le Sous-Traitant est tenu de traiter les données à caractère personnel des salariés, préposés et représentants légaux du Responsable de Traitement, transmises par ce dernier.

Tenant compte de l'évolution de la réglementation en vigueur, le présent avenant a pour objet de déterminer les conditions dans lesquelles le Sous-traitant traite les données à caractère personnel communiquées par le Responsable de Traitement et les conditions dans lesquelles ils en assurent chacun la sécurité dans le respect de la réglementation applicable.

En conséquence de quoi il a été convenu et arrêté ce qui suit :

1 RESPECT DE LA REGLEMENTATION EN VIGUEUR

Dans le cadre du traitement de données à caractère personnel, objet des présentes, les parties s'engagent à respecter la réglementation en vigueur son compte du respect de la confidentialité des informations confidentielles.

2 DESCRIPTION DU TRAITEMENT

Le Sous-Traitant est autorisé à traiter pour le compte du Responsable de Traitement les données à caractère personnel nécessaires pour fournir les prestations définies dans le Contrat.

La nature des opérations réalisées sur les données est la collecte, l'enregistrement, la conservation, l'extraction, la consultation, l'utilisation, et la suppression.

Les données à caractère personnel traitées sont :

- Les données d'identification des contacts commercial, technique ou de facturation (telles que nom, prénom, numéro de téléphone personnel, coordonnées électroniques).
- Les adresses IP si l'utilisateur utilise sa connexion personnelle à titre professionnelle.
- Les données d'authentification des utilisateurs dans le réseau professionnel du Client.
- Toute trace personnelle identifiables via les Logs confiés à SNS SECURITY.
- Dans le cas d'un test d'intrusion confié à SNS SECURITY, tout document ou toute donnée présente dans le réseau professionnelle du client inclus dans la cible du test (adresses IP choisies par le Client). Toute donnée personnelle sensible pouvant être récolté sans être identifié comme tel à la récupération de celle-ci fera l'objet d'une destruction immédiate après en avoir informer le client. Les données sensibles correspondent aux informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique

Les catégories de personnes concernées sont les salariés et préposés du Responsable de Traitement ainsi que ses représentants légaux ainsi que tout utilisateur du réseau professionnel du Responsable de Traitement éventuellement confié à SNS SECURITY.

3 OBLIGATIONS DU SOUS-TRAITANT VIS-A-VIS DU RESPONSABLE DE TRAITEMENT

Le Sous-Traitant accepte et garantit ce qui suit:

- 3.1 il traitera les données à caractère personnel pour le compte exclusif du Responsable de Traitement conformément à la réglementation en vigueur, aux finalités déterminées par lui, aux instructions transmises par écrit par ce dernier, et conformément aux présentes clauses ;
- 3.2 il dispose des mesures techniques et d'organisation liées à la sécurité spécifiées en annexe afin de traiter les données à caractère personnel communiquées ;
- 3.3 il communiquera par écrit sans retard au Responsable de Traitement :
 - toute demande contraignante de divulgation des données à caractère personnel émanant d'une autorité de maintien de l'ordre, sauf disposition contraire, telle qu'une interdiction de caractère pénal visant à préserver le secret d'une enquête policière ;
 - toute obligation 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 français, avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;
 - tout accès fortuit ou non autorisé ;
 - toute demande reçue directement des personnes concernées sans répondre à cette demande, à moins qu'il n'ait été autorisé par écrit à le faire ;
 - toute impossibilité ou incapacité de se conformer aux instructions du Responsable de Traitement notamment en raison d'une potentielle violation de la réglementation l'empêchant de remplir ses obligations, auquel cas, ce dernier a le droit de suspendre et/ou de résilier les présentes ;
- 3.4 dans le cadre de leur obligation de collaboration, le Sous-Traitant répondra dans les meilleurs délais aux demandes de renseignements du Responsable de Traitement relatives à ses opérations de traitement, il aidera le Responsable de Traitement pour la réalisation d'analyses d'impact relatives à la protection des données et pour la réalisation de la consultation préalable de la CNIL sur demande de ce dernier ;
- 3.5 il garantit la confidentialité des données à caractère personnel traitées dans le cadre des présentes et il veillera à ce titre, à ce que son personnel autorisé à traiter les données à caractère personnel s'engage également à respecter la confidentialité ou qu'il soit soumis à une obligation légale de confidentialité et reçoive la formation nécessaire en matière de protection des données à caractère personnel ;
- 3.6 il s'engage à prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut.

4 OBLIGATIONS DU RESPONSABLE DE TRAITEMENT VIS-A-VIS DU SOUS-TRAITANT

Le Responsable de Traitement accepte et s'assure de ce qui suit :

- 4.1. il a chargé, et chargera le Sous-Traitant de traiter les données à caractère personnel selon des instructions et pour des finalités conformes au RGPD, au droit français et aux présentes clauses pendant toute la durée des présentes ;
- 4.2. le Sous-Traitant présente les garanties suffisantes de sécurité pendant toute la durée des présentes, conformément à la réglementation en vigueur ;
- 4.3. il veillera au respect des mesures de sécurité spécifiées en annexe des présentes, et d'une manière générale, il s'assure du respect d'une sécurité suffisante en vertu de la réglementation en vigueur, afin de protéger les données à caractère personnel contre une destruction fortuite ou illicite, une perte fortuite, une altération, une divulgation ou un accès non autorisé, notamment lorsque le traitement suppose la transmission de données par réseau, et contre toute autre forme illicite de traitement et il s'assure que ce niveau de sécurité est adapté aux risques liés au traitement et à la nature des données à protéger, eu égard au niveau technologique et au coût de mise en œuvre du traitement ;

4.4. il fournira au Sous-Traitant les données visées à l'article 2 des présentes ;

4.5. il documentera par écrit et transmettra au Sous-Traitant toute instruction supplémentaire concernant le traitement des données qui se rajouterait aux instructions initiales ;

4.6. il supervise le traitement, y compris en réalisant des audits et inspections auprès du Sous-Traitant.

5 SOUS-TRAITANCE ULTERIEURE

Le Sous-Traitant peut faire appel à un autre sous-traitant (ci-après, le « Sous-Traitant Ulérieur ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le Responsable de Traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres Sous-Traitants Ulérieurs. Cette information doit indiquer les activités de traitement sous-traitées, l'identité et les coordonnées du Sous-Traitant Ulérieur et les dates du contrat de sous-traitance. Le Responsable de Traitement dispose d'un délai de 10 jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le Responsable de Traitement n'a pas émis d'objection pendant le délai convenu, étant précisé que toute objection du Responsable de Traitement devra être justifiée.

En tout état de cause, le Sous-Traitant Ulérieur est tenu de respecter les obligations des présentes pour le compte et selon les instructions du Responsable de Traitement.

Il appartient au Sous-Traitant initial de s'assurer que le Sous-Traitant Ulérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière que le traitement réponde aux exigences du RGPD et de la loi française relative à la protection des données.

Le Sous-Traitant initial demeure pleinement responsable à l'égard du Responsable de Traitement en cas de manquement, par le Sous-Traitant Ulérieur, aux obligations en matière de protection des données qui lui incombent conformément audit accord écrit et à la réglementation en vigueur.

Plus spécifiquement, en cas de recours à un Sous-Traitant Ulérieur impliquant un transfert de données vers un pays tiers ne présentant pas de garanties suffisantes au sens du RGPD, le Sous-Traitant devra conclure avec le Sous-Traitant Ulérieur un contrat conforme à la réglementation en vigueur.

La responsabilité civile du Sous-Traitant Ulérieur est limitée à ses propres activités de traitement conformément aux présentes.

6 DROITS DES PERSONNES CONCERNEES

6.1. Droit d'information des personnes concernées

Il appartient au Responsable de Traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

6.2. Exercice des droits des personnes

Dans la mesure du possible, le Sous-Traitant doit aider le Responsable de Traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage), et droit de définir des directives relatives au sort de ses données après son décès.

Lorsque les personnes concernées exercent auprès du Sous-Traitant des demandes d'exercice de leurs droits, le Sous-Traitant doit adresser ces demandes dès réception par courrier électronique à rgpd@sns-security.fr.

7 VIOLATION DE DONNEES A CARACTERE PERSONNEL

7.1. Notification des violations de données à caractère personnel au Responsable de Traitement

Le Sous-Traitant notifie au Responsable de Traitement toute violation de données à caractère personnel dans un délai maximum de 48 heures après en avoir pris connaissance et par tout moyen écrit. Cette notification est

accompagnée de toute documentation utile afin de permettre au Responsable de Traitement, si nécessaire, de notifier cette violation à la CNIL.

7.2. Notification des violations de données à caractère personnel à la CNIL et communication à la personne concernée

Le Responsable de Traitement fera son affaire personnelle de la notification de la violation de données à caractère personnel à la CNIL ainsi que de sa communication aux personnes concernées. Le Sous-Traitant reconnaît ainsi qu'il n'est pas autorisé à réaliser ces notification et communication au nom et pour le compte du Responsable de Traitement.

8 RESPONSABILITES

Si l'une des parties répare la totalité du préjudice subi par une personne concernée, elle peut en réclamer la part de réparation correspondant à la part de responsabilité de l'autre partie dans le dommage.

Sans préjudice des éventuelles actions en réparation intentées par la personne concernée ou des éventuelles sanctions prononcées par la CNIL ou toute autre autorité compétente, chaque partie est responsable envers l'autre des dommages qu'elle lui cause par suite d'un manquement aux présentes clauses.

La responsabilité entre les parties se limite au dommage effectif subi, à l'exclusion des dommages indirects tels que préjudice commercial, atteinte à l'image de marque, trouble commercial quelconque, perte de bénéfices, de gains et/ou de profits, perte de chance, perte de clients. En tout état de cause, le montant des dommages-intérêts qui pourraient être mis à la charge du Sous-Traitant en application des présentes, tout préjudice confondu et cumulé, si sa responsabilité était engagée, ne pourra excéder une somme correspondant au montant HT du contrat conclu avec le Responsable de Traitement et effectivement payé par lui. Tout dommage subi par un tiers est un dommage indirect, et ne donne pas lieu en conséquence à indemnisation.

9 DELEGUES A LA PROTECTION DES DONNEES

Les parties se communiquent mutuellement le nom et les coordonnées de leur délégué à la protection des données, s'ils en ont désigné un conformément à l'article 37 du RGPD.

10 REGISTRE DES ACTIVITES DE TRAITEMENT

Les parties déclarent tenir un registre écrit de toutes les catégories d'activités de traitement effectuées en vertu des présentes comprenant :

- le nom et les coordonnées du Responsable de Traitement, du Sous-Traitant et des éventuels Sous-Traitants Ulérieurs et, le cas échéant, du délégué à la protection des données de chacun d'eux ;

- les catégories de traitements effectués ;

- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du RGPD, les documents attestant de l'existence de garanties appropriées ;

- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :

- la pseudonymisation et le chiffrement des données à caractère personnel ;

- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

11 RESILIATION

En cas de manquement par une partie à l'une de ses obligations, l'autre partie peut temporairement suspendre le contrat jusqu'à ce qu'il soit remédié au manquement ou que le contrat soit résilié.

Le Sous-Traitant pourra résilier le contrat, sans préjudice des autres droits qu'il pourrait faire valoir à l'encontre du Responsable de Traitement, dans les cas suivants :

- la suspension du transfert conformément à l'article 11.1. des présentes, pendant une durée supérieure à un mois ;
- en cas de violation par le Responsable de Traitement d'une de ses obligations prévues aux articles 1, 2, 4, 6, 9, 10 des présentes.

Cette résiliation interviendra après mise en demeure adressée par courrier recommandée avec demande d'avis de réception, demeurée sans effet quinze (15) jours calendaires après sa réception.

12 SORT DES DONNEES APRES LA CESSATION DES RELATIONS CONTRACTUELLES

Les parties conviennent qu'au terme des présentes, le Sous-Traitant et le Sous-Traitant Ulérieur, pour qui il se porte fort, s'engagent à transmettre l'ensemble des données à caractère personnel au nouveau sous-traitant désigné par le Responsable de Traitement, dans les délais qu'il conviendra au Sous-Traitant et sur un support de son choix. Cette transmission doit s'accompagner de la destruction de toutes les copies existantes.

Le Responsable de Traitement reconnaît expressément que la destruction des données ou de leurs copies ne pourra être demandée en cas d'obligation de conservation légale ou réglementaire à laquelle serait soumis le Sous-Traitant ou le Sous-Traitant Ulérieur, et ce, dans la limite des données et de la durée strictement nécessaires au respect de ladite obligation.

Dans ce cas, le Sous-Traitant garantit qu'il assurera la confidentialité des données à caractère personnel transférées et qu'il ne traitera plus activement ces données. Il se porte également fort que le Sous-Traitant Ulérieur respectera également cette obligation.

Le Sous-Traitant et le Sous-Traitant Ulérieur, pour qui le Sous-Traitant se porte fort, devront justifier à toute date du respect des obligations prévues au paragraphe 1 sur demande du Responsable de Traitement et/ou de la CNIL.

13 REPRESENTATION, MEDIATION, JURIDICTION ET COOPERATION AVEC LES AUTORITES DE CONTROLE

Les parties ont connaissance et acceptent que la personne concernée a le droit de se faire représenter par une association ou un autre organisme à but non lucratif si elle en exprime le souhait conformément à la réglementation en vigueur.

Les parties acceptent que la personne concernée puisse demander réparation du préjudice subi dans les conditions de l'article 8.1 des présentes, soit en soumettant le litige à la médiation d'une personne indépendante ou, le cas échéant, de l'autorité de contrôle ; soit en portant le litige devant les tribunaux de l'Etat membre où le Responsable de Traitement est établi.

Les parties conviennent que le choix effectué par la personne concernée ne remettra pas en cause le droit procédural ou matériel de cette dernière d'obtenir réparation conformément à d'autres dispositions du droit national ou international.

14 RECONNAISSANCE ET DECLARATIONS

Les parties s'engagent à ne pas modifier les présentes clauses. Les parties restent libres d'inclure d'autres clauses à caractère commercial qu'elles jugent nécessaires, à condition qu'elles ne contredisent pas les présentes clauses.

Les clauses sont régies par le droit de l'Etat membre où le Responsable de Traitement est établi, à savoir le droit français.

Les présentes sont rédigées en langue française, dans le cas où il serait traduit en une ou plusieurs langues, seul le texte français ferait foi en cas de litige.

15 STIPULATIONS FINALES

Toutes les autres clauses, charges et conditions du contrat conclu entre les parties mentionnées en préambule des présentes, demeurent inchangées.

Il est formellement convenu que toute tolérance ou renonciation d'une des parties, dans l'application de tout ou partie des engagements prévus aux présentes, quelles qu'en ait pu être la fréquence et la durée, ne saurait valoir modification des présentes, ni générer un droit quelconque.

La nullité ou l'inapplicabilité de l'une quelconque des stipulations des présentes n'emportera pas nullité des autres stipulations qui conserveront toute leur force et leur portée. Cependant, les parties pourront d'un commun accord, convenir de remplacer la ou les stipulations invalidées.

16 MESURES DE SECURITE

16-1 Gouvernance en matière de protection des données

Gouvernance des données intégrée au CODIR avec COPILS. Le RSSI pilote la sécurité au SI. Le DPO s'assure de l'intégrité, de l'usage et de la destruction des données personnelles collectées.

16-2 Politique interne formalisée de protection des données

Une Politique RGD est mise en place intégrant un suivi par l'intermédiaire d'un registre de traitement. Des clauses sont intégrées dans les contrats de travail avec également une charte informatique, une charte administrateur, et une PSSI incluses dans la politique

16-3 Désignation d'un délégué à la protection des données pour l'ensemble des traitements mis en œuvre

Un DPO est désigné et accessible à l'adresse mail ci-après : rgpd@sns-security.fr

16-4 Information, conseil et sensibilisation des salariés procédant au traitement, en matière de protection des données à caractère personnel

- Politique de Sécurité des Systèmes d'Information (PSSI),
- Charte informatique,
- Clauses contractuelles,
- Campagnes de sensibilisation régulières,
- Surveillance et prévenance le cas échéant

16-5 Certification, en matière de protection de la vie privée, approuvée ou délivrée par une autorité de contrôle en matière de protection des données personnelles

SNS SECURITY a pour cœur d'activité la création et la mise en œuvre de solutions en matière de cybersécurité. SNS applique les préconisations en la matière de protection de la vie privée et est labellisé Cybermalveillance.

16-6 Procédure permettant d'identifier un traitement de données personnelles, en amont de la mise en œuvre de celui-ci par les métiers de SNS Security

Segmentation du traitement des données personnelles selon les domaines d'activités stratégiques de SNS Security et en fonction des dossiers.

16-7 Intégration des principes dans le cadre des activités

Intégration du principe du Privacy by design / by default et de minimisation.

16-8 Procédure permettant d'identifier les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées, pour lesquels il est nécessaire de réaliser une analyse d'impact relative à la protection des données

Procédure intégrée dans la PSSI de SNS SECURITY.

16-9 Procédure encadrant le recours, par votre entité, à des sous-traitants RGD dans la mise en œuvre des traitements

Limitation du recours au sous-traitants et contractualisation très stricte le cas échéant comportant des obligations de sécurité conformes aux exigences de SNS SECURITY.

16-10 Mesures de sécurité physiques ou matérielles

- Portes fermées à toutes les entrées
- Système de contrôle d'accès nominatif.
- Télésurveillance,
- Systèmes d'alarme de sécurité
- Badges nominatifs par salle

16-11 Mesures de sécurité logiques ou logicielles

- Équipements réseaux et sécurité redondés
- SOC interne
- Logiciels de sécurité dans les postes de travail

16-12 Politique de gestion des mots de passe

- Systèmes de sécurité informatique exigeant que les utilisateurs individuels se connectent avec un nom d'utilisateur unique
- Systèmes de sécurité informatique exigeant l'utilisation de mots de passe contraignants
- Systèmes de sécurité informatique exigeant l'utilisation de l'authentification multifactorielle
- Changement de mot de passe obligatoire à intervalle fixe
- Verrouillage automatique des terminaux et appareils informatiques après une période de non-utilisation, avec un mot de passe requis pour « rallumer » le terminal

- Puissant chiffrement/hachage des bases de données de mots de passe
- Utilisation de mots de passe très contraignants pour les comptes à privilège
- Mise en place de profils utilisateurs avec principe du moindre privilège gérés dans l'Active Directory
- Gestion des droits et des profils dans les logiciels externes

16-13 Politique d'authentification des utilisateurs et de gestion des habilitations
Politique très stricte intégrée dans la PSSI et les chartes informatique et administrateur

16-14 Encadrement contractuel opposable aux salariés et/ou tiers intervenant sur le SI

- PSSI
- Charte informatique,
- Clauses incluses dans les contrats de travail (RGPD, confidentialité...)
- Règlement Intérieur,
- Clause RGPD
- Normes ISO 27001 demandées aux fournisseurs

16-15 Certifications ou labels en matière de sécurité informatique
Label Cybermalveillance et démarche PASSI / ISO 27001

16-16 Réalisation des audits de sécurité interne et/ou externe
Audits interne réguliers et compétences internalisées.

16-17 Accessibilité depuis Internet ou par des systèmes d'information externes des serveurs utilisés pour le traitement des données (pas de firewall, pas de DMZ)

Les serveurs ne sont pas accessibles sur internet hormis l'extranet faisant l'objet d'une restriction DMZ et accessible via un firewall sécurisé.

16-18 Comptes pour l'accès aux serveurs ou applications gérant le traitement des données
Utilisation de comptes nominatifs à des fins de traçabilité et de sécurisation du système d'information.

16-19 Anti-virus sur les serveurs et/ou les postes de travail
Mise à jour automatique de l'antivirus et des patterns est réalisée en temps réel avec une sécurisation par EPP / EDR. Surveillance quotidienne des mises à jour disponible.

16-20 Des journaux de connexion et d'utilisation existent-ils ? Si oui, quelle est la durée de conservation (ex : 6 mois - 1 an) ?
Logs sur l'ensemble du système d'information avec des durées de conservation différenciées selon les systèmes (1 an ou 1 trimestre).

16-21 Quelles mesures de sécurité sont mises en œuvre s'agissant du stockage des données ?
Des mesures de sécurité sont mises en place tel que les équipements réseaux redondés, les backups quotidiens, les serveurs sécurisés...

16-22 Les données que vous traitez sont-elles stockées, même temporairement, hors de l'UE ?
Les données ne sont pas stockées hors de l'UE.

16-23 Lieux de stockage des données
Le serveur principal est situé dans le datacenter Jaguar tier3 (Marseille) avec des backups effectués au siège social de SNS SECURITY.

16-24 Gestion des clés cryptographiques et chiffrement.
La gestion des clés cryptographiques est distincte de celle des données chiffrées. Les données sont chiffrées par nos outils

16-25 Autres mesures tendant à la sécurisation des échanges
Tunnel VPN IPSEC, Chiffrement des flux (SSL/TLS), Chiffrement des postes de travail, Limitation des échanges par messagerie au profit d'espaces sécurisés, Mise en place de systèmes d'évaluation des vulnérabilités, de technologies de protection contre les menaces, de gestion des mises à jour, et de procédures de surveillance conçues pour identifier, évaluer, atténuer et protéger contre les menaces identifiées sur la sécurité, les virus et autres codes malveillants.

16-26 Récupération des données en cas de problème
Un plan de continuité d'activité est déclenché par la cellule de crise (CODIR et COPIL) et des Backups sont réalisés via la réplication entre le siège et le datacenter Jaguar.

16-27 Transfert des données

Les activités de traitement sur les données dans les cas suivants n'impliquent pas des transferts de données en dehors de l'UE et de l'EEE ni pour l'utilisation de nos services, ni pour l'administration ou la gestion de nos services, ni pour le support ou la maintenance de nos services.

16-28 Informations relatives à la gestion des réclamations et exercice des droits
Procédure de gestion des droits des personnes (Recueil du consentement, portabilité des données, droit d'opposition, droit d'accès et de rectification...).

16-29 Informations relatives à la gestion des violations de données
Procédure visant à remonter tout incident pouvant constituer une violation de données à caractère personnel (Procédure de Traitement des Incidents de sécurité intégrée dans la PSSI) et procédure de gestion et/ou notification et/ou information des personnes concernées en cas de violation de données à caractère personnel.