



Conditions générales relatives à Kaspersky Hosted Security

Les présentes conditions générales (CG) régissent la fourniture du système Kaspersky Hosted Security (KHS) par Kaspersky Lab à l'utilisateur.

1 Définitions et Interprétations

Dans les présentes CG, les mots ci-dessous ont les définitions suivantes :

Client : signifie la société ou autre entité légale à laquelle est fourni le KHS.

Kaspersky Lab : signifie pour les besoins du présent document le Groupe Kaspersky.

Kaspersky Hosted Email Security : signifie « Kaspersky Hosted Email Security » tel que décrit dans la version la plus récente de la description du système KHS.

Kaspersky Hosted Web Security : signifie « Kaspersky Hosted Web Security » tel que décrit dans la version la plus récente de la description du système KHS.

Kaspersky Hosted Security (KHS) : signifie « Kaspersky Hosted Email Security » et/ou « Kaspersky Hosted Web Security », ou toute combinaison des deux, tel que décrit dans la version la plus récente de la description du système KHS.

Description de KHS : signifie les dispositions contenant les descriptions techniques du système KHS, dont la version la plus récente est jointe aux présentes CG.

Logiciel malveillant (malware) : signifie un programme informatique rédigé dans l'intention explicite de détruire ou de corrompre les données et/ou le code d'un ordinateur cible, et/ou de réduire sa facilité d'utilisation, et/ou d'y permettre un accès abusif.

Frais mensuels : signifie 1/12 du prix payé par un Client pour une année d'utilisation du KHS, ou le prix payé par un Client pour un mois d'utilisation du KHS.

Relais ouvert : signifie un serveur SMTP configuré de façon à permettre à chacun sur Internet d'envoyer des e-mails en passant par ce serveur, et pas seulement des messages en provenance/direction d'utilisateurs ou domaines connus.

Nombre d'utilisateurs autorisés : signifie le nombre d'utilisateurs inscrits sur le Certificat de licence.

Portail : signifie une configuration Web utilisée par un Client pour gérer le KHS et obtenir des rapports.

Certificat de licence : signifie le certificat confirmant l'octroi d'une licence KHS, la période d'abonnement et le nombre d'utilisateurs autorisés, auquel sont jointes les présentes CG.

Période d'abonnement : signifie la période payée par un Client, durant laquelle il utilise le KHS ; elle est inscrite sur le Certificat de licence.

Date de départ : signifie la date d'activation du KHS inscrite sur le Certificat de licence.

Spam : signifie des messages de masse non sollicités et envoyés sans discrimination.

Utilisateur : signifie (i) une entité physique ou virtuelle (dans le cas des boîtes de messagerie partagées) disposant d'une boîte de messagerie d'entreprise avec un ou plusieurs pseudonymes associés, et dont la fonction Kaspersky Hosted Email Security scanne les e-mails et/ou (ii) une entité physique ou virtuelle (dans le cas d'ordinateurs partagés) qui peut accéder aux ressources Internet et dont la fonction Kaspersky Hosted Web Security traite les contenus Web.

Contenu Web : signifie toutes données et toutes requêtes de données traitées par la fonction Kaspersky Hosted Web Security, y compris, sans aucune limitation, celles auxquelles on peut accéder en utilisant les protocoles Internet HTTP et FTP.

2 Domaine d'application des présentes CG

2.1 Kaspersky Lab octroie au Client les droits d'utilisation du système KHS selon les conditions générales définies dans les présentes.

2.2 Ces CG s'appliquent à la fourniture du système KHS par Kaspersky Lab. Les Pièces et Annexes concernent présentement le KHS décrit ici et indiqué dans le Certificat de licence. Toutes CG différentes de celles-ci qui seraient indiquées sur la commande du Client ou dans tous autres documents du Client seront rejetées et resteront nulles et sans effet à moins d'avoir été approuvées expressément par écrit par les deux parties.

3 Durée

- 3.1 Les présentes CG prennent effet à la Date de départ et, sous réserve de la clause 4, resteront en vigueur durant toute la Période d'abonnement.

4 Résiliation

- 4.1 Kaspersky Lab est en droit de résilier les CG avec effet immédiat en notifiant le Client dans le cas où le Client aurait omis de s'acquitter de son règlement du KHS dans les conditions requises ;
- 4.1.1 Kaspersky Lab contrôlera l'utilisation du système KHS par le Client. Si le nombre réel d'Utilisateurs dépasse le nombre autorisé, Kaspersky Lab sera en droit, à sa seule convenance, de résilier les CG avec effet immédiat en notifiant le Client ou de facturer en proportion et avec règlement immédiat le nombre d'Utilisateurs supplémentaires.
- 4.2 Sans préjudice d'aucun autre droit conféré par les présentes CG, chacune des parties peut résilier les CG avec effet immédiat par préavis écrit à l'autre partie si cette autre partie viole les présentes CG dans de grandes proportions et (si une telle violation peut être réparée) omet d'y apporter réparation dans un délai de trente (30) jours après en avoir été avisé par préavis écrit.
- 4.3 Dès résiliation par le Client au titre de la clause 4.2 pour violation des présentes CG par Kaspersky Lab, la proportion de frais payés par le Client correspondant à la Période d'abonnement non utilisée après résiliation sera remboursée au Client.
- 4.4 Dès résiliation des CG en conséquence d'une violation par le Client des présentes CG, le droit du Client à utiliser le KHS prendra fin avec effet immédiat et toutes les factures deviendront échues et exigibles.
- 4.5 Les clauses des présentes CG indiquées ci-dessous survivront après résiliation : les clauses 1, 7, 8, 9, 10, 13, 14 et 20.

5 Fourniture du KHS

- 5.1 Kaspersky Lab s'engage à déployer des efforts raisonnables pour fournir le KHS au Nombre autorisé d'Utilisateurs durant la Période d'abonnement.
- 5.2 Kaspersky Lab se réserve le droit, avant l'inscription au système Kaspersky Hosted Email Security et à tout moment durant la fourniture du système Kaspersky Hosted Email Security, de tester si le système de messagerie du Client fonctionne en mode Relais ouvert. Si les systèmes du Client s'avèrent fonctionner en mode Relais ouvert, Kaspersky Lab en informera le Client et se réserve le droit de suspendre immédiatement tout ou partie du système Kaspersky Hosted Email Security jusqu'à ce que le problème ait été résolu.
- 5.3 Si, à un quelconque moment, la fourniture du système KHS au Client compromettrait la sécurité offerte par le KHS, pour des raisons, sans aucune limitation, de piratage, attaques de refus de service, inondation (afflux de requêtes en ligne) ou autres activités malveillantes en provenance ou en direction du réseau du Client, Kaspersky Lab se réserve le droit de suspendre immédiatement tout ou partie du KHS jusqu'à ce que le problème ait été résolu. Dans ce cas, Kaspersky Lab informera promptement le Client et travaillera avec le Client, qui se doit de coopérer, pour résoudre un tel problème de façon à rétablir le KHS dès que possible.
- 5.4 Si, à un moment quelconque, le Client utilise le système Kaspersky Hosted Email Security pour distribuer des spams, Kaspersky Lab se réserve le droit de suspendre immédiatement tout ou partie du système Kaspersky Hosted Email Security jusqu'à ce que le problème ait été résolu.
- 5.5 Si le KHS est suspendu ou résilié pour quelque raison que ce soit, Kaspersky Lab annulera tout changement de configuration effectué après l'inscription au KHS et il sera de la responsabilité du Client d'entreprendre tous les changements de configuration nécessaires pour réacheminer correctement son trafic de messagerie et/ou son trafic Web.
- 5.6 Sous réserve de la législation en vigueur, Kaspersky Lab peut fournir le KHS en utilisant toute installation matérielle, en tout point du monde, et peut, à tout moment, en transférer la fourniture d'une installation à l'autre.
- 5.7 Afin de remplir ses obligations, Kaspersky Lab peut modifier le KHS et toute documentation y afférente s'il y a lieu, à savoir, sans aucune limitation, d'effectuer tous changements répondant aux normes du secteur ainsi qu'à des impératifs juridiques, commerciaux ou techniques. Tout changement deviendra effectif dès la publication par Kaspersky Lab d'une nouvelle Description de KHS sur le Portail.

6 Obligations du Client

- 6.1 Le Client reconnaît que le KHS sera fourni avec les paramètres standards par défaut de Kaspersky Lab et qu'il incombe entièrement au Client de configurer le KHS au moyen du Portail de sorte qu'il puisse répondre à ses propres exigences. Les représentants de Kaspersky Lab peuvent aider à configurer le KHS de façon à ce qu'il fonctionne de façon optimale. Kaspersky Lab se réserve le droit de modifier les paramètres du client dans des situations d'urgence afin de préserver la qualité du système KHS pour un Client ou plus.
- 6.2 Le Client fournira s'il y a lieu à Kaspersky Lab toutes données techniques et toutes autres informations pouvant être raisonnablement requises par Kaspersky Lab afin de fournir le KHS au Client. Toutes informations fournies par le Client seront complètes, précises et données de bonne foi. Ces informations seront traitées comme des Informations confidentielles selon les présentes Conditions Générales.
- 6.3 Le Client ne doit pas utiliser son système de messagerie :
- 6.3.1 en mode Relais ouvert ;
- 6.3.2 pour envoyer des spams.



- 6.4 Le Client reconnaît que les informations envoyées en direction et en provenance du Client doivent passer par le KHS et le Client s'engage en conséquence à :
- 6.4.1 se conformer à toute législation en vigueur concernant l'utilisation d'Internet et de la messagerie électronique ;
 - 6.4.2 n'utiliser le KHS qu'à des fins professionnelles légitimes, à savoir l'envoi et la réception de messages électroniques professionnels et personnels/l'utilisation de contenus Web par ses employés ;
 - 6.4.3 ne pas utiliser le KHS pour transmettre des spams ;
 - 6.4.4 se conformer s'il y a lieu aux protocoles et normes publiés sur Internet et adoptés par la majorité des utilisateurs d'Internet ;
 - 6.4.5 indemniser Kaspersky Lab de toutes obligations financières envers des tiers résultant de la transmission d'informations par le Client via le KHS.
- 6.5 Le Client s'engage à ne pas utiliser le KHS dans le cadre d'activités illégales et à indemniser Kaspersky Lab pour tous coûts, pertes et dépenses pouvant être encourus par Kaspersky Lab en raison desdites activités illégales, à savoir mais sans aucune limitation :
- 6.5.1 des infractions civiles ou criminelles de droits de propriété intellectuelle, à savoir mais sans aucune limitation, des droits d'auteur, des marques de commerce et des brevets ; ou
 - 6.5.2 la transmission ou la publication de documents obscènes, indécents ou pornographiques ; ou
 - 6.5.3 l'exécution de toute infraction criminelle selon la législation en vigueur ; ou
 - 6.5.4 la transmission ou la publication de tout document diffamatoire, offensant, abusif ou menaçant, ou
 - 6.5.5 la transmission ou la publication de tout document enfreignant la loi Data protection Act de 1998 ou toute législation similaire en vigueur ;
 - 6.5.6 l'utilisation du système KHS d'une quelconque manière qui viole ou enfreigne les droits de tout individu, organisation ou société.
- 6.6 Le Client est autorisé uniquement à ajouter des domaines de messagerie détenus par le Client ou dont il possède la preuve juridique avançant qu'il est en droit d'ajouter ces domaines au système Kaspersky Hosted Security. Kaspersky Lab se réserve le droit de vérifier l'appartenance du domaine ou le droit au domaine avant la mise en service du KHS.
- 6.7 Afin que ne subsiste aucun doute, toute violation des clauses 6.3-6.6 incluses constituera une infraction substantielle des CG. Si le Client omet de se conformer à toute obligation définie dans les clauses 6.3-6.6, sans préjudice de ses autres droits stipulés dans les CG ou le Contrat, Kaspersky Lab peut à tout moment suspendre l'utilisation du KHS par le Client jusqu'à ce que le Client ait résolu le problème.
- 6.8 Le KHS est fourni au Client pour son usage personnel et le Client ne doit le revendre à aucun tiers.

7 Garantie

Kaspersky Lab exercera toutes les compétences et prendra toutes les précautions raisonnablement nécessaires pour fournir le KHS dans les limites autorisées par la loi. Les conditions qui précèdent remplacent et excluent toutes autres garanties, conditions et autres dispositions expresses et implicites, à savoir, mais sans aucune limitation, toutes garanties de qualité et d'adaptation à un usage spécifique.

8 Responsabilité limitée

TOUTES REVENDICATIONS LICITES DU CLIENT CONCERNANT LA DISPONIBILITE ET/OU LA QUALITE DU KHS AINSI QUE TOUTES AUTRES RECLAMATIONS AYANT TRAIT AU KHS SONT SOUMISES AUX LIMITATIONS SUIVANTES :

- 8.1 LA RESPONSABILITE DE KASPERSKY LAB POUR DES PERTES ET DOMMAGES SUBIS PAR LE CLIENT (Y COMPRIS LA PERTE DE DONNEES) OU LES RECLAMATIONS DE TIERS FAISANT SUITE A DES RECLAMATIONS DU CLIENT CAUSEES PAR LA NON-CONFORMITE DU KHS A LA DESCRIPTION DU KHS (EX. INDISPONIBILITE, DEFECTUOSITES OU PROBLEMES DE QUALITE DU KHS) CONSECUTIVE A UNE NEGLIGENCE DE KASPERSKY LAB, SES EMPLOYES OU SES AGENTS EST LIMITEE A UN MONTANT MAXIMUM CORRESPONDANT AU TOUT DERNIER MONTANT REEL DEVANT ETRE PAYE PAR LE CLIENT POUR LE KHS SUR UNE PERIODE D'UN (1) AN. CETTE LIMITE S'APPLIQUE A CHAQUE EVENEMENT OU SERIE D'EVENEMENTS ASSOCIES.
- 8.2 SONT EXCLUES TOUTES DEMANDES DE REMBOURSEMENT DU CLIENT CORRESPONDANT A UNE PERTE DE PROFIT / PERTE DE VENTE / PERTE DE REPUTATION / PERTE DE CONTRATS ET/OU DE CLIENTS, OU DE DEDOMMAGEMENT A LA SUITE DE LA PERTE DE DONNEES.
- 8.3 KASPERSKY LAB NE PEUT ETRE TENUE POUR RESPONSABLE DE DOMMAGES PROVOQUES PAR LE CLIENT SUITE AU NON-RESPECT DES CG, OU A L'UTILISATION DU KHS D'UNE FAÇON NON CONFORME AUX CG.
- 8.4 LES LIMITATIONS ET EXCLUSIONS QUI PRECEDENT NE S'APPLIQUENT PAS DANS LES CAS SUIVANTS :
 - 8.4.1 DECES, DOMMAGE CORPOREL OU MALADIE D'UNE PERSONNE,
 - 8.4.2 TOUTE RESPONSABILITE NE POUVANT ETRE LIMITEE OU EXCLUE PAR LA LOI,



8.4.3 L'INDEMNITE POUR VIOLATION DE DROITS DE PROPRIETE INTELLECTUELLE SPECIFIEE A LA CLAUSE 14.

8.5 **KASPERSKY LAB ATTIRE TOUT PARTICULIEREMENT L'ATTENTION DU CLIENT SUR LE FAIT QUE LE KHS REPOSE SUR L'UTILISATION DES MESURES ELECTRONIQUES ET DES ALGORITHMES DECRITS DANS LES CG ET LA DESCRIPTION DU KHS :**

8.5.1 EU EGARD A L'ETAT DES DEVELOPPEMENTS TECHNOLOGIQUES, CES MESURES SERONT MAINTENUES PAR KASPERSKY LAB A UN NIVEAU RAISONNABLE AFIN DE GARANTIR QUE, NORMALEMENT, SEULS LES E-MAILS CONTENANT DES VIRUS OU CONSIDERES COMME DES SPAMS SONT DETECTES COMME « POSITIFS » ET DOIVENT PAR CONSEQUENT ETRE BLOQUES ET MIS EN QUARANTAINE CONFORMEMENT AUX DISPOSITIONS CONTENUES DANS LES PRESENTES CG ET DANS LA DESCRIPTION DU KHS. TOUTEFOIS, IL N'EST PAS POSSIBLE DE GARANTIR QUE, DANS CERTAINS CAS ET DANS CERTAINES CIRCONSTANCES (POUVANT INCLURE LA CONFIGURATION DU CLIENT), DES E-MAILS DESIRES PAR LE CLIENT OU NON INFECTES PAR DES VIRUS NE SOIENT PAS BLOQUES ET MIS EN QUARANTAINE (« FAUSSEMENT POSITIFS »). LE CLIENT ACCEPTE DONC L'OBLIGATION DE VERIFIER REGULIEREMENT LA LISTE DE QUARANTAINE DU KHS. KASPERSKY LAB REJETTE TOUTE RESPONSABILITE DE PERTES ET/OU DE DOMMAGES RESULTANT DE LA NON-TRANSMISSION DE CES E-MAILS FAUSSEMENT POSITIFS, AINSI QUE TOUTE RESPONSABILITE DANS LE CAS OU DES E-MAILS « FAUSSEMENT POSITIFS » AURAIENT ETE DETRUIIS AU BOUT DE 30 JOURS A PARTIR DE LA DATE OU ILS ONT ETE TRANSMIS.

9 Confidentialité

9.1 Chaque partie s'engage, pendant la durée de la Période d'abonnement et sur les trois (3) ans qui suivront, (sous réserve des clauses 9.2 et 9.3) à garder confidentielle et à ne pas utiliser à son propre usage ni, sans le consentement écrit préalable de l'autre partie, divulguer à un tiers toute information d'une nature confidentielle (y compris des secrets commerciaux et des informations d'une valeur commerciale) pouvant avoir été divulguée à, ou venir à la connaissance de, cette partie en provenance de l'autre partie ou de ses sous-traitants (« Informations confidentielles »). Les obligations ci-dessus ne s'appliquent pas aux informations connues du public, ou si une partie peut prouver que les informations lui étaient déjà connues au moment où elles ont été divulguées, ou si elles viennent ensuite à être connues du public autrement que par une violation des présentes CG, ou si elles sont ensuite obtenues légalement d'un tiers sans aucune obligation de les garder confidentielles. Aucune des parties ni aucun de ses sous-traitants ne seront réputés violer la présente clause si la loi exige de divulguer les Informations confidentielles, sous réserve que cette partie ait d'abord donné à l'autre un préavis minimum de 14 (quatorze) jours avant de les divulguer comme l'exige la loi.

9.2 Dans la mesure où elle met en œuvre et/ou respecte les dispositions des présentes CG, chaque partie peut divulguer les Informations confidentielles à ceux de ses employés et sous-traitants qui ont besoin d'y accéder à des fins professionnelles, sous réserve qu'avant cette divulgation, chaque partie fasse prendre conscience à ses employés et sous-traitants de ses obligations de confidentialité en vertu des présentes CG, et fasse en sorte qu'ils les observent.

9.3 Kaspersky Lab reconnaît que le contenu de tous les e-mails envoyés ou reçus au/du Client et tout contenu Web ou requête de contenu Web sont confidentiels. Kaspersky Lab, en dehors de ses obligations contractuelles, n'inspectera pas ni n'utilisera le contenu des e-mails, contenus Web, ou requêtes de contenus Web du Client. Dans le cadre normal de la fourniture du KHS, tout accès par Kaspersky Lab et toute lecture et/ou copie d'e-mails et/ou de leurs pièces jointes, de contenus Web et de requêtes d'accès à des contenus Web ne seront effectués qu'aux seules fins d'assurer le KHS. Toutes données seront traitées comme strictement confidentielles.

9.4 Toutefois, Kaspersky Lab se réserve le droit d'utiliser le contenu véhiculant un virus de ces e-mails et/ou de leurs pièces jointes / des contenus Web et des données de la connexion Internet utilisées par le Client, aux seules fins de :

9.4.1 préserver et améliorer les performances et l'intégrité du KHS,

9.4.2 respecter les exigences réglementaires, législatives ou contractuelles, et

9.4.3 mettre ce contenu véhiculant un virus à la disposition des octroyeurs de licences KHS afin qu'ils développent plus avant et améliorent le KHS.

9.5 En outre, Kaspersky Lab se réserve le droit d'utiliser les e-mails contenant des spams et/ou leurs pièces jointes envoyés au domaine du Client et pour lesquels aucune adresse e-mail n'est configurée sur le serveur du Client, aux seules fins de :

9.5.1 préserver et améliorer les performances et l'intégrité du KHS,

9.5.2 respecter les exigences réglementaires, législatives ou contractuelles, et

9.5.3 mettre ces e-mails contenant des spams à la disposition des octroyeurs de licences KHS afin qu'ils développent plus avant et améliorent le KHS.

10 Confidentialité des données et réglementation concernant le pouvoir d'enquête

10.1 Le Client prendra toutes les mesures nécessaires pour s'informer, ainsi que tous ses employés, sur leurs responsabilités eu égard à toutes les lois et/ou réglementations en vigueur sur la protection des données et, du fait que Kaspersky Lab n'exerce aucun contrôle ni aucune influence sur le contenu des e-mails/contenus Web traités par le KHS, le Client doit défendre Kaspersky Lab et l'indemniser entièrement si un tiers intente une procédure à la suite de la violation par le Client de la loi Data Protection Act de 1998 ou de toute législation similaire en vigueur.



- 10.2 Le Client doit donner tout consentement et toute indication nécessaires au traitement, au stockage et à l'utilisation des données personnelles nécessaires pour la fourniture du KHS selon les présentes CG.
- 10.3 Quand, et si, des données personnelles seront traitées durant la fourniture du KHS, elles le seront exclusivement en conformité avec les présentes CG, et seulement aux fins et dans la mesure nécessaire à la fourniture du KHS.
- 10.4 Le Client garantit qu'il s'est conformé à toutes les règles et réglementations en vigueur afférentes à la mise en œuvre d'une procédure d'accès à la messagerie électronique/à Internet dans son organisation et, le cas échéant, a obtenu le consentement de ses employés ou de son comité d'entreprise pour la mise en œuvre de KHS, notamment pour l'interception, la lecture, la copie ou le filtrage des e-mails et/ou de leurs pièces jointes/des contenus Web.
- 10.5 Si la législation en vigueur l'exige, le Client doit informer (par exemple par un bandeau sur les e-mails) toute personne utilisant un système de communications couvert par le KHS que les communications transmises via ce système peuvent être interceptées et contrôlées, et indiquer les objectifs d'une telle interception et d'un tel contrôle. Aucune des parties ne doit utiliser, ni exiger de l'autre partie qu'elle utilise à des fins illicites une quelconque donnée obtenue via le KHS.

11 Force Majeure

Les obligations de chacune des parties au titre des présentes CG doivent être suspendues et, dans la mesure où cette partie rencontre des obstacles inévitables l'empêchant ou lui permettant difficilement de remplir ces obligations pour des causes échappant à son contrôle, à savoir mais sans aucune limitation : grèves, contre-grèves, guerre, terrorisme, émeute, mouvement populaire, dommage volontaire, respect dû à une loi ou un ordre, une réglementation ou une directive gouvernementale, accident, incendie, inondation, tempête, coupures d'alimentation ou pannes de réseaux ou connexions externes d'importance.

12 Suspension

En aucun cas une suspension du KHS autorisée par les présentes CG, autre qu'une suspension due à une défaillance de Kaspersky Lab, ne prolongera la Période d'abonnement.

13 Droits de propriété intellectuelle

Le Client reconnaît que le KHS et tous développements, systèmes, concepts, modes d'emploi, documentations et autres informations contenus dans le KHS constituent la propriété intellectuelle exclusive et/ou des secrets commerciaux de Kaspersky Lab ou de ses partenaires, et que Kaspersky Lab et ses partenaires, s'il y a lieu, sont protégés par le droit civil et criminel et par la législation sur les droits d'auteur, les secrets commerciaux, les marques et les brevets de la Fédération russe, de l'Union européenne, des États-Unis d'Amérique et de tous autres pays ainsi que par les traités internationaux. Les présentes CG n'accordent au Client aucun droit à ladite propriété intellectuelle, y compris toutes marques de commerce ou de service de Kaspersky Lab et/ou de ses partenaires (« marques de commerce »). L'utilisation autorisée d'une marque de commerce ne confère au Client aucun droit de propriété sur cette marque de commerce. Le détenteur des droits et/ou ses partenaires possèdent et conservent tout droit, titre et intérêt sur/dans le KHS, y compris sans aucune limitation toutes corrections d'erreurs, mises à jour ou autres modifications du KHS, qu'elles soient effectuées par Kaspersky Lab ou un tiers, ou tous droits d'auteur, brevets, droits sur les secrets commerciaux, marques de commerce et autres droits de propriété intellectuelle y afférents. L'utilisation par le Client du KHS ne transfère au Client aucun titre de propriété intellectuelle du KHS, et le Client n'acquerra aucun droit au KHS sauf disposition expresse contraire dans les présentes CG. Sauf indication contraire dans les présentes, ces CG n'accordent au Client aucun droit de propriété intellectuelle sur le KHS, et le Client reconnaît que la licence du produit KHS définie ultérieurement et octroyée par ces CG ne donne au Client que le droit d'utiliser le KHS en vertu de celles-ci. Kaspersky Lab se réserve tous droits non expressément octroyés au Client dans ces CG.

14 Droits de propriété intellectuelle d'un tiers

- 14.1 Si le KHS enfreint tous droits de propriété intellectuelle d'un tiers, Kaspersky Lab défendra et/ou règlera toute réclamation d'un tiers sous réserve que :
- 14.1.1 le Client doive promptement, dès qu'il a connaissance d'une telle réclamation, en notifier par écrit Kaspersky Lab ;
 - 14.1.2 le Client donne à Kaspersky Lab tout contrôle sur une telle action ou de telles procédures judiciaires ;
 - 14.1.3 le Client coopère pleinement avec Kaspersky Lab et lui fournisse toute assistance qu'il peut raisonnablement requérir pour régler et/ou défendre une telle action ou de telles procédures judiciaires (aux frais de Kaspersky Lab) ;
 - 14.1.4 la liquidation de tous dépens et/ou dommages-intérêts incombe à Kaspersky Lab.
- 14.2 Si le KHS enfreint tous droits de propriété intellectuelle d'un tiers, Kaspersky Lab, à sa seule appréciation, doit remplacer le KHS par un produit non contrefait, ou peut résilier immédiatement les présentes CG par avis écrit au Client, en quel cas sont exclues toutes demandes de règlement de dommages-intérêts mais le Client est en droit d'être remboursé de la proportion des frais payés pour le reste de la Période d'abonnement.
- 14.3 Les dispositions des clauses 14.1 et 14.2 ci-dessus ne s'appliquent à aucune contrefaçon résultant de :
- 14.3.1 l'utilisation du KHS de façon non conforme à celle autorisée par les présentes CG ; ou
 - 14.3.2 la combinaison du KHS avec tout produit et/ou service d'un tiers ou toute modification effectuée par le Client sans le consentement écrit préalable de Kaspersky Lab, si une telle combinaison ou modification entraîne la contrefaçon.



15 Publicité

Le Client et Kaspersky Lab conviennent que chacune des parties peut divulguer le fait qu'elles entretiennent une relation commerciale. Kaspersky Lab est notamment en droit d'inscrire le Client dans sa liste de Clients de référence. Toutefois, aucun autre détail de cette relation commerciale ni du Contrat ou des présentes CG ne doit être divulgué sans le consentement exprès de l'autre partie.

16 Modifications

- 16.1 Ni une modification, ni une variante, ni l'annulation de ces CG ne prendra effet si elle n'est formulée par écrit. Ceci couvre la modification ou l'annulation de la présente clause elle-même.
- 16.2 Nonobstant la clause 16.1, Kaspersky Lab se réserve le droit de modifier les détails techniques du KHS dans la mesure où une telle modification ne porte pas atteinte à la qualité du KHS. Si une telle modification, pour des raisons fondées, est inacceptable par le Client, les deux parties sont en droit de résilier les CG avec effet immédiat. Toute demande de règlement de dommages-intérêts est exclue dans ce cas mais le Client est en droit d'être remboursé de la proportion de frais payés pour le reste de la Période d'abonnement.

17 Cession

Le Client n'est pas en droit de céder les présentes CG ni une quelconque créance à un tiers sans le consentement écrit préalable de Kaspersky Lab.

18 Divisibilité des CG

Si une quelconque disposition de ces CG est, ou devient, nulle et non avenue, le reste de ces CG reste en vigueur. Les parties dans ce cas s'engagent à remplacer la disposition nulle et non avenue par une autre disposition valide correspondant le plus possible à celle-ci ainsi qu'à l'objectif du contrat.

19 Pièces jointes

La Description du KHS et les Pièces jointes aux présentes sont une partie importante des présentes CG.

20 Législation en vigueur et tribunal compétent

- 20.1 Les présentes CG sont régies par et doivent être interprétées selon la législation en vigueur dans le pays où le KHS a été acquis.
- 20.2 Les parties conviennent de façon irrévocable que les tribunaux d'Angleterre ont une compétence non exclusive pour régler tout litige ou toute réclamation résultant de ces CG ou y afférent(e).



Description de Kaspersky Hosted Security

1 Résumé

Kaspersky Lab est une société spécialisée dans les produits de sécurité relatifs aux technologies de l'information (IT). Nous proposons le système Kaspersky Hosted Security (KHS) pour mettre en application les procédures de sécurité des entreprises dans le domaine IT. Le KHS protège les e-mails (Kaspersky Hosted Email Security) et les sites Web (Kaspersky Hosted Web Security). Le présent document décrit toutes les parties du KHS, sans discrimination, y compris les parties de cette suite de produits qui ne sont pas incluses dans la licence du Client.

La présente Description du KHS ne s'applique présentement que si le Client a acquis une licence pour la partie correspondante du KHS, et en vertu des présentes Conditions Générales auxquelles est annexée cette Description du KHS. Les mots en majuscules mais non définis dans cette Description du KHS ont la signification définie dans les CG.

2 Définitions

- 2.1 **Grappe désignée (designated cluster)** signifie une grappe de serveurs désignée pour fournir le KHS au Client de façon non exclusive.
- 2.2 **Jour ouvrable normal** signifie du lundi au vendredi, à l'exclusion des jours fériés sur le lieu de résidence habituel de Kaspersky Lab.
- 2.3 **En dehors des heures ouvrables** signifie toute heure ne faisant pas partie des heures ouvrables.
- 2.4 **Garanties** couvre l'ensemble des paramètres de travail du KHS définis dans la présente Description du KHS.
- 2.5 **Heures ouvrables** signifie les heures de bureau d'un jour ouvrable normal.

3 Disponibilité du KHS

- 3.1 Le KHS est disponible 24 h sur 24, 7 jours sur 7, auprès des Centres d'opérations de Kaspersky Lab. Le KHS est contrôlé en termes de disponibilité, de capacité et de taux d'utilisation des ressources du réseau. Cette surveillance étroite permet d'effectuer des ajustements réguliers sur le KHS pour garantir son efficacité maximale.
- 3.2 Le KHS est hautement disponible et évolutif. Tout le trafic fait l'objet d'un équilibrage des charges entre les centres de données appartenant à diverses zones géographiques. Chaque centre de données est créé pour offrir une disponibilité maximale. Dans le cas improbable d'une panne d'un centre de données complet, le centre de sauvegarde des données Client prend le relais sans perturbation notable du trafic acheminé.
- 3.3 Les garanties ne s'appliquent PAS :
 - 3.3.1 si le Client utilise le KHS pour distribuer des spams ;
 - 3.3.2 si le système de messagerie électronique du Client fonctionne en mode Relais ouvert ;
 - 3.3.3 à moins que le Client n'utilise la technologie de Grappe désignée ;
 - 3.3.4 durant la Période d'essai ;
 - 3.3.5 si la configuration système du Client n'est pas conforme à l'ensemble des directives de configuration standard de Kaspersky Lab publiées périodiquement ;
 - 3.3.6 durant les périodes de Maintenance planifiée (sous réserve de la clause 4) et les périodes de non-disponibilité dues à des cas de force majeure, des actes ou des omissions du Client ou d'un tiers ;
 - 3.3.7 durant toute période de suspension du KHS par Kaspersky Lab en vertu des CG ;
 - 3.3.8 en cas de panne de l'infrastructure du Client ou de la connexion Internet ;
 - 3.3.9 en cas d'indisponibilité du KHS causée par des informations incorrectes fournies par le Client ;
 - 3.3.10 pour des raisons hors du contrôle de Kaspersky Lab définies dans les CG.

4 Maintenance planifiée

- 4.1 Maintenance planifiée signifie les périodes de maintenance pouvant causer une perturbation du KHS du fait de la non-disponibilité d'une (ou de) Grappe(s) ou de leurs composants. Dans la mesure du possible, la maintenance planifiée sera exécutée sans affecter le KHS. Ceci sera généralement obtenu en exécutant la maintenance planifiée durant des périodes anticipées de faible trafic d'e-mails, et au cours d'étapes conçues pour éviter tout effet préjudiciable sur les Clients. Durant les périodes de maintenance planifiée, le trafic peut être détourné vers les parties du réseau non soumises à la maintenance afin de minimiser toute perturbation du KHS.
- 4.2 La Maintenance planifiée n'aura pas lieu entre 8 h 00 et 18 h 00 (dans le fuseau horaire où se trouve la grappe de serveurs).
- 4.3 Le Client sera notifié par Kaspersky Lab de la Maintenance planifiée, dans un délai non inférieur à sept (7) jours avant celle-ci. Kaspersky Lab peut informer le Client en envoyant un e-mail et/ou en publiant un message d'alerte sur le Portail.



4.4 Si une maintenance d'urgence susceptible d'affecter le KHS est nécessaire, Kaspersky Lab s'efforcera d'en informer le Client et peut afficher un message d'alerte sur le Portail.

5 Portail Web

5.1 Partie intégrante du KHS. Il s'agit d'un outil de configuration Web, gestion et génération de rapports, désigné ici comme le Portail. Après qu'un Client s'est abonné au KHS, il lui est affecté un nom d'utilisateur et un mot de passe afin d'ouvrir à son administrateur le plein accès au compte du Client sur le Portail, où peuvent être configurés ses procédures et paramètres. Le Portail donne également accès à des statistiques, des rapports et aux e-mails placés en quarantaine.

5.2 Le Portail est disponible en anglais, en français, en allemand et en russe.

6 Assistance technique

6.1 Kaspersky Lab fournit une assistance technique 24 h sur 24, 7 jours sur 7. L'assistance technique peut être assurée par téléphone ou par e-mail.

6.2 Durant les Heures ouvrables, l'assistance est disponible en anglais, en français, en allemand et en russe. L'assistance En dehors des heures ouvrables est disponible en anglais.

6.3 Kaspersky Lab vise et s'appliquera raisonnablement à répondre à tous les appels téléphoniques dans un délai de 60 secondes, et à commencer à travailler sur chaque cas dans un délai d'une heure.

6.4 Les Clients recevront un numéro de ticket pour chaque appel au service d'assistance.

6.5 Coordonnées des personnes à contacter :

	Adresse e-mail	Numéro de téléphone
Benelux (hollandais)	KHS-Support@kaspersky.com	+31(0)307529539
Danemark, Finlande, Norvège et Suède (danois, finnois, norvégien, suédois, anglais)	KHS-Support@kaspersky.com	+46(0)85 785 3031
Allemagne, Autriche, Suisse (allemande)	KHS-Support@kaspersky.com	+49(0)84198189760
France (en français)	KHS-Support@kaspersky.com	+33(0)141398933
Italie	KHS-Support@kaspersky.com	
Russie (en russe)	KHS-Support@kaspersky.com	+7 (495) 9567800
Espagne (espagnol)	KHS-Support@kaspersky.com	+34 913983566
Royaume-Uni (en anglais)	KHS-Support@kaspersky.com	+44(0)8454590165
Autres pays (en anglais)	KHS-Support@kaspersky.com	+7 (495) 9567800

6.6 Tous les appels entrants seront consignés et les priorités suivantes leur seront affectées (voir matrice ci-dessous) :

Priorité	Problème	Réponse durant les Heures ouvrables	Réponse En dehors des heures ouvrables	Résolution
I	Indisponibilité du KHS ou incident majeur	1 heure	1 heure	Dès que raisonnablement possible mais sans jamais dépasser 24 heures
II	Perte partielle du KHS mais traitement du trafic non interrompu	2 heures	12 heures	Dès que raisonnablement possible, tout étant fait pour résoudre le problème dans les deux Jours ouvrables normaux
III	Problèmes techniques ou de configuration	4 heures	Jour ouvrable suivant	Accord entre le Client et l'équipe d'assistance
IV	Questions standards, assistance en cas de quarantaine, problèmes liés aux informations	1 Jour ouvrable normal	Jour ouvrable suivant	Accord entre le Client et l'équipe d'assistance



7 Demande d'un avoir

- 7.1 Si, d'après la Description du KHS, le Client estime qu'il a droit à une compensation, il peut soumettre une Demande d'avoir. « Demande d'avoir » signifie que le Client doit notifier KHS-Support@kaspersky.com en indiquant comme objet « Credit Request » (sauf indication contraire donnée par Kaspersky Lab) en respectant le délai spécifié dans la Description du KHS. Sous réserve d'une vérification d'admissibilité par Kaspersky Lab, cette dernière créditera le Client selon les dispositions appropriées de la présente Description du KHS. Aucun des remboursements des frais déjà payés ne sera effectué. LE CLIENT RECONNAÎT QUE LES ENREGISTREMENTS NE SONT CONSERVÉS QUE SUR UN NOMBRE DE JOURS LIMITÉ ET PAR CONSÉQUENT QU'AUUCUNE DEMANDE D'AVOIR SOUMISE HORS DU DÉLAI SPÉCIFIÉ NE SERA PRISE EN CONSIDÉRATION ET NE DONNERA LIEU À UN AVOIR.



Kaspersky Hosted Email Security

8 Définitions

- 8.1 **Faux négatif** signifie un Spam et/ou un e-mail infecté par un Logiciel malveillant mais non identifié comme un Spam et/ou un Logiciel malveillant ;
- 8.2 **Faux positif** signifie un e-mail légitime incorrectement identifié/capturé comme un Spam et/ou un Logiciel malveillant.
- 8.3 **Logiciel malveillant connu** signifie un Logiciel malveillant (malware) qui a déjà été identifié et dont la signature ou la définition a été publiée afin de permettre sa détection ultérieure dans le trafic, par Kaspersky Lab ou l'un de ses partenaires technologiques dont la technologie anti-malware est utilisée dans le système Kaspersky Hosted Email Security. Cette détection a lieu au moins vingt (20) minutes avant l'analyse (scan) par le KHS de l'e-mail infecté par ce Logiciel malveillant.

9 Présentation

- 9.1 Le système Kaspersky Hosted Email Security effectue l'analyse anti-spam et anti-malware des e-mails et des pièces jointes pour déterminer s'ils contiennent des Logiciels malveillants (malware) ou des Spams. Il filtre aussi bien les e-mails en entrée que les e-mails en sortie.
- 9.2 Le système Kaspersky Hosted Email Security est disponible pour les Clients dont les systèmes de messagerie sont connectés en permanence à Internet avec une adresse IP fixe. Il ne peut être fourni aux Clients dont les systèmes de messagerie sont connectés à Internet via des lignes commutées ou des lignes RNIS ou dont l'adresse IP est allouée dynamiquement.
- 9.3 Tout le trafic de messagerie sera routé en utilisant SMTP via une Grappe (cluster) désignée.
- 9.4 Kaspersky Lab propose une liaison cryptée opportuniste entre le centre de données assigné et le serveur de messagerie du Client en utilisant TLS (si le serveur de messagerie du Client prend en charge le cryptage TLS).
- 9.5 Kaspersky Hosted Email Security scanne les e-mails jusqu'à 100 Mo. Les e-mails d'une taille supérieure à 100 Mo sont rejetés avec le code d'erreur approprié.
- 9.6 Pour tous les e-mails en entrée, le système vérifie la réputation IP de l'émetteur. Les e-mails provenant d'une source de mauvaise réputation (telle qu'un spammeur) sont ralentis ou rejetés au niveau connexion pour minimiser leur impact sur KHS.
- 9.7 Le Client peut ajouter des domaines de messagerie au Portail pour en filtrer les e-mails.
- 9.8 Kaspersky Hosted Email Security offre diverses options de traitement soumises à l'utilisateur. Le Client peut définir s'il accepte : toutes les adresses électroniques pour un domaine ajouté automatiquement ; seulement les adresses électroniques définies manuellement ; seulement les adresses électroniques confirmées comme valides par une autorisation SMTP ; seulement les adresses électroniques confirmées comme valides par le Service effectuant un appel via LDAP vers le serveur d'annuaire du Client.

10 Kaspersky Hosted Email Security. Anti-spam

- 10.1 La fonctionnalité anti-spam utilise plusieurs technologies pour garantir que la plus grande proportion possible de spams soit détectée.
- 10.2 Le moteur anti-spam est réglé continuellement pour identifier les e-mails qui sont des spams (« Spams ») de façon quasiment certaine, et ceux qui sont probablement des spams (« Spams probables »).
- 10.3 Le Client peut configurer des dispositifs séparés pour le traitement des Spams et des Spams probables. Ceux disponibles sont : aucune action ; taguer le champ Objet ; supprimer l'e-mail ; mettre l'e-mail en quarantaine.
- 10.4 Liste d'émetteurs approuvés : Peuvent être ajoutés à la liste d'émetteurs approuvés des adresses électroniques, des domaines ou des adresses IP de serveurs de messagerie. Le contenu de ces entrées ne sera pas scanné pour y détecter des Spams et sera transmis à moins d'être filtré par une autre partie de la procédure (par exemple anti-malware).
- 10.5 Liste d'émetteurs bloqués : Peuvent être ajoutés à la liste d'émetteurs bloqués des adresses électroniques, des domaines ou des adresses IP de serveurs de messagerie. Les e-mails en provenant seront rejetés avec le message d'erreur approprié.
- 10.6 Les entrées des listes approuvées et bloquées peuvent être configurées dans le KHS en utilisant le Portail.
- 10.7 La fonctionnalité de définition de Groupes permet de regrouper des utilisateurs ou des domaines de messagerie afin d'y appliquer des procédures et de générer des rapports. À chaque Groupe peut être appliquée une procédure différente.

11 Kaspersky Hosted Email Security. Anti-malware

- 11.1 Afin d'assurer une sécurité maximale, la fonctionnalité anti-malware (ou anti-logiciels malveillants) du KHS se compose de plusieurs technologies anti-malware. Les moteurs anti-malware utilisent des technologies de reconnaissance de forme ou de signature ainsi que des algorithmes heuristiques (le moteur Kaspersky BitHunt) pour protéger les Clients des logiciels malveillants du type « jour zéro ».



- 11.2 Kaspersky BitHunt est un moteur sophistiqué et exclusif de Kaspersky Lab et il n'est disponible qu'au travers de KHS. Il protège les Clients des logiciels malveillants du type « jour zéro » en identifiant les e-mails malveillants avant la technologie de reconnaissance de forme.
- 11.3 Lorsqu'un Logiciel malveillant est détecté dans un e-mail, un dispositif ou une action doit être sélectionné(e). Le dispositif peut être configuré par le Client. Les options sont : attacher une étiquette dans le champ Objet ; supprimer l'e-mail ; supprimer la pièce jointe ; mettre l'e-mail en quarantaine.

12 Kaspersky Hosted Email Security. Continuité de l'activité

- 12.1 Kaspersky Lab surveille continuellement le nombre d'e-mails de chaque Client dans les files d'attente de ses serveurs de messagerie. Lorsqu'une file d'attente d'e-mails montante est détectée pour un domaine connecté, Kaspersky Lab teste l'aptitude du serveur de réception de messagerie à recevoir les e-mails. Si Kaspersky Lab est dans l'incapacité de délivrer un e-mail au serveur de messagerie du Client, Kaspersky Lab stocke cet e-mail entrant pendant sept (7) jours au maximum. Durant cette période, Kaspersky Lab tente périodiquement de délivrer les e-mails dans sa file d'attente et, dès que possible, le fait de façon contrôlée.
- 12.2 Kaspersky Lab offre au Client l'accès à tous les e-mails entrants mis en file d'attente parce que le serveur de messagerie du Client n'a pas été en mesure de les recevoir via le Portail. Ces e-mails peuvent être consultés dans le Portail.

13 Kaspersky Hosted Email Security. Traitement des pièces jointes

- 13.1 La fonctionnalité de traitement des pièces jointes permet de contrôler la taille, le type et les noms des pièces jointes aux e-mails.
- 13.1.1 Kaspersky Hosted Email Security peut faire la distinction entre documents, fichiers exécutables, archives, fichiers graphiques, audio, vidéo et autres types de fichiers.
- 13.1.2 Un champ de texte libre est disponible pour l'ajout de texte (une sous-chaîne) qui pourra être comparé de la façon suivante aux pièces jointes : noms correspondant à cette sous-chaîne ; extension contenant cette sous-chaîne ; extension correspondant à cette sous-chaîne ; nom ou extension contenant cette sous-chaîne ; nom ou extension correspondant à cette sous-chaîne.
- 13.2 Le Client peut configurer la façon de traiter les fichiers cryptés par un mot de passe. Les dispositifs disponibles pour les règles ci-dessus concernant les pièces jointes sont : aucune action ; taguer le champ Objet ; supprimer l'e-mail ; mettre l'e-mail en quarantaine.

14 Kaspersky Hosted Email Security. Quarantaine

- 14.1 Tous les e-mails en quarantaine sont stockés 30 jours puis supprimés automatiquement.
- 14.2 L'utilisateur peut accéder sans risque à tous les e-mails en quarantaine et les gérer via le Portail.
- 14.3 La section Quarantaine du Portail offre une possibilité de recherche de texte dans les champs Objet ; De ; et À . À la suite de cette recherche, les e-mails répondant aux critères seront affichés avec l'heure, l'émetteur, le récepteur, l'objet, le statut et la taille de l'e-mail.
- 14.4 Les e-mails dans la page de résultats peuvent être ouverts, supprimés ou libérés.
- 14.5 Pour chaque e-mail en quarantaine, des informations complémentaires d'en-tête détaillées sont disponibles en cliquant sur l'email et sur le bouton « en-tête » (header).
- 14.6 Les listes d'émetteurs bloqués ou approuvés du domaine ou de l'émetteur peuvent être modifiées en cliquant sur les boutons correspondants dans la vue de la quarantaine.
- 14.7 Les utilisateurs peuvent libérer un e-mail en quarantaine via le rapport de quarantaine.

15 Kaspersky Hosted Email Security. Rapports

- 15.1 Des rapports peuvent être générés à l'intérieur du Portail. Cette fonctionnalité est disponible selon les parties du KHS dont le Client a acquis la licence.
- 15.2 Tous les rapports sont disponibles sous forme graphique (HTML) ou de PDF.
- 15.3 Les rapports peuvent être générés pour des périodes de temps et pour des domaines spécifiés, pour des boîtes de messagerie, des groupes de boîtes de messagerie et des groupes de domaines.
- 15.4 Le rapport de synthèse du compte (account summary report) affiche le nombre de transactions, de catégories et de volumes.
- 15.5 Les rapports peuvent porter sur les e-mails, les utilisateurs, les Logiciels malveillants (malware), les Spams, l'hameçonnage (phishing) et les e-mails mis en quarantaine.
- 15.6 Un journal détaillé est disponible dans la zone Rapports (reporting) du Portail.



- 15.7 Les rapports sur les e-mails montrent les nombres d'e-mails et le volume du trafic.
- 15.8 Les rapports indiquent le trafic entrant et sortant.
- 15.9 Le rapport sur la quarantaine (QR, quarantine report) fournit à chaque utilisateur un rapport indiquant tous ses e-mails mis en quarantaine. Ce rapport peut être requis en utilisant le Portail. Il peut être transmis par e-mail ou exécuté lors de la connexion au Portail.
- 15.9.1 Fréquence des rapports : une fois par jour, par semaine, par mois et selon un intervalle défini par l'utilisateur.
- 15.9.2 Période sur laquelle porte le rapport : aujourd'hui, hier, cette semaine, la semaine dernière, ce mois-ci, le mois dernier.
- 15.9.3 Informations contenues dans le QR : période sur laquelle porte le rapport, nombre d'e-mails, e-mails en quarantaine et raison pour laquelle chacun a été mis en quarantaine
- 15.10 En parcourant le rapport sur la quarantaine, les utilisateurs peuvent activer la libération d'e-mails mis en quarantaine.
- 15.11 Les rapports sont générés en temps réel.

16 Kaspersky Hosted Email Security. Garanties

- 16.1 Disponibilité. Kaspersky Lab garantit une durée de disponibilité pour Kaspersky Hosted Email Security qui est de 99,999 %.
- 16.2 Pour ce système, la Disponibilité est définie comme l'aptitude, mesurée par Kaspersky Lab, à établir une session SMTP sur le port 25 de la Grappe (cluster) désignée. Cette garantie ne s'applique que si toute la configuration nécessaire est exécutée par le Client afin de permettre à la Grappe désignée de recevoir les e-mails entrants du Client et d'accepter les e-mails sortants 24 h sur 24, 7 jours sur 7.
- 16.3 Si, sur n'importe quel mois calendaire, la Disponibilité venait à être inférieure à 99,999 %, le Client pourrait être en droit de recevoir un avoir du pourcentage suivant :

Disponibilité par mois calendaire	Avoir en pourcentage des Frais mensuels
< 99,999 % mais >= 99,99 %	10 %
< 99,99 % mais >= 99 %	25 %
< 99 % mais >= 98 %	50 %
< 98 %	100 %

- 16.4 Si la Disponibilité devenait inférieure à quatre-vingt-dix-huit pour cent (98 %) durant un mois calendaire donné, le Client serait en droit de résilier immédiatement les présentes CG et de recevoir un remboursement en proportion des frais couvrant la Durée spécifiée non utilisée après résiliation.
- 16.5 Si le Client estime qu'il a droit au recours stipulé en 16.3, il devra envoyer une Demande d'avoir (credit request) dans un délai de quatorze (14) jours après la fin du mois calendaire en question.
- 16.6 Temps de latence. Kaspersky Lab garantit que la durée moyenne de traitement des e-mails (mesurée par Kaspersky Lab en envoyant toutes les 5 minutes des e-mails à la Grappe désignée) sera inférieure à 60 secondes. Si, durant un mois calendaire, le Temps d'attente dépassait les délais indiqués dans le tableau ci-dessous, le Client serait en droit de recevoir un avoir du pourcentage suivant :

Durée moyenne de transfert par mois dans les deux sens	Avoir en pourcentage des Frais mensuels
>1 mn mais <= 1 mn 30 s	25 %
>1 mn 30 s mais <= 2 mn	50 %
>2 mn mais <= 2 mn 30 s	75 %
>2 mn 30 s	100 %

- 16.7 Si le Client estime qu'il a droit au recours stipulé en 16.6, il devra envoyer une Demande d'avoir dans un délai de quatorze (14) jours après la fin du mois calendaire en question.
- 16.8 Détection des Logiciels malveillants (malware) : Kaspersky Lab détectera 100 % de tous les Logiciels malveillants connus dans le trafic traité par le KHS.
- 16.9 Si un ou plusieurs exemplaires de Logiciels malveillants connus scannés par le KHS ne sont pas détectés sur n'importe quel mois calendaire et ont entraîné l'infection des systèmes du Client, Kaspersky Lab paiera directement tous les coûts de main-



d'œuvre raisonnables et encourus, avec justificatifs à l'appui, pour éliminer ces Logiciels malveillants du réseau du Client jusqu'à un montant maximal équivalent à 3 mois de Frais mensuels. Pour recevoir un remboursement de ce coût, le Client doit envoyer une Demande d'avoir à Kaspersky Lab dans un délai de 14 jours à compter de la violation de garantie. Cette Demande d'avoir doit identifier le Logiciel malveillant et la source d'infection, en démontrant que le KHS n'a pas filtré ce Logiciel malveillant, et doit inclure un justificatif des coûts encourus et dont le remboursement est demandé.

- 16.10 Les systèmes du Client sont réputés être infectés si un Virus contenu dans le trafic reçu via le KHS a été activé dans les systèmes du Client, soit automatiquement, soit par une intervention manuelle.
- 16.11 La garantie contre les Logiciels malveillants contenue dans les clauses 16.8 et 16.9 ne s'appliquera pas dans les conditions suivantes :
- 16.11.1 le Logiciel malveillant était dans un e-mail qui n'a pu être scanné ou analysé par le KHS (ex. des e-mails cryptés ou protégés par des mots de passe) ;
 - 16.11.2 Kaspersky Lab a notifié le Client immédiatement après la transmission d'un e-mail contenant ce Logiciel malveillant et le Client a omis de prendre les mesures appropriées ;
 - 16.11.3 le Logiciel malveillant a été libéré de la quarantaine par le Client ;
 - 16.11.4 auto-infection par le Client.
- 16.12 Taux de détection des Spams : Kaspersky Lab garantit de détecter 98 % de tous les Spams entrants et d'agir conformément à la procédure configurée par le Client via le Portail.
- 16.13 Si, durant un quelconque mois calendaire, le taux de détection des Spams, calculé comme étant le nombre de Spams incorrectement identifiés divisé par la somme du nombre de Spams correctement identifiés et du nombre de Spams faussement négatifs, est inférieur à celui indiqué dans le tableau, le Client a droit à l'avoir en pourcentage suivant :

Taux de détection des Spams durant le mois calendaire	Avoir en pourcentage des Frais mensuels
< 98 % mais >= 97 %	25 %
< 97 % mais >= 96 %	50 %
< 96 % mais >= 95 %	75 %
< 95 %	100 %

- 16.14 Pour recevoir cet avoir, le Client devra envoyer les e-mails suspectés être faussement négatifs à KHS-Support@kaspersky.com, dans une pièce jointe préservant tous les en-têtes d'origine des e-mails, dans un délai de 5 (cinq) jours après réception de chaque e-mail. Kaspersky Lab fera son enquête et vérifiera si cet e-mail est oui ou non un Spam faussement négatif, en consignnant le résultat. À la fin du mois calendaire, si le Client estime que le nombre de Spams faussement négatifs lui donne droit à un avoir selon la clause 16.13, le Client devra envoyer une Demande d'avoir à Kaspersky Lab dans un délai de 14 (quatorze) jours après la fin du mois calendaire respectif.
- 16.15 La garantie ne s'applique pas dans les conditions suivantes :
- 16.15.1 le Client n'a pas mis en œuvre la méthode préconisée par Kaspersky Lab (best practice) quand il a configuré le KHS ;
 - 16.15.2 l'e-mail n'a pas été envoyé à une adresse légitime.
- 16.16 Un taux inférieur de capture de Spams de 95 % s'applique aux e-mails contenant les jeux de caractères arabes et asiatiques. Si ce taux de capture de Spams devient inférieur à 95 %, le Client aura droit à un avoir représentant 25 % de ses Frais mensuels. Si ce taux de capture de Spams devient inférieur à 90 %, le Client aura droit à un avoir représentant 100 % de ses Frais mensuels.
- 16.17 Spams faussement positifs. Si le taux de capture de Spams faussement positifs grimpe pour atteindre 0,0004 % sur l'ensemble du trafic d'e-mails du Client sur n'importe quel mois calendaire, le Client peut être en droit de recevoir un avoir selon le tableau ci-dessous.

Taux de Spams faussement positifs durant le mois calendaire	Avoir en pourcentage des Frais mensuels
>0,0004 % mais <= 0,004 %	25 %
> 0,004 % mais <= 0,04 %	50 %
>0,04 % mais <= 0,4 %	75 %
>0,4 %	100 %



- 16.18 Pour remplir les conditions requises pour un avoir selon la clause 16.13, le Client devra envoyer les e-mails suspectés d'être Faussement positifs sous forme de pièce jointe à KHS-Support@kaspersky.com dans un délai de 5 (cinq) jours après réception de chaque e-mail. Kaspersky Lab fera son enquête et vérifiera si cet e-mail est oui ou non Faussement positif, en consignnant le résultat. À la fin du mois calendaire, si le Client estime que le nombre d'e-mails Faussement positifs confirmés sur le mois calendaire lui donne droit à un avoir selon la clause 16.17, le Client devra envoyer une Demande d'avoir à Kaspersky Lab dans un délai de 14 (quatorze) jours après la fin du mois calendaire respectif.
- 16.19 Les e-mails qui suivent ne constitueront pas des e-mails Faussement positifs dans le cadre de la présente garantie :
- 16.19.1 les e-mails ne constituant pas des e-mails professionnels légitimes ;
 - 16.19.2 si l'émetteur de l'e-mail est sur la liste de blocage du Client ;
 - 16.19.3 les e-mails envoyés depuis une source compromise et rejetés selon la clause 9.6 ;
 - 16.19.4 les e-mails envoyés depuis une machine se trouvant sur une liste d'émetteurs bloqués d'un tiers ;
 - 16.19.5 les e-mails envoyés à plus de 20 destinataires et dont au moins 80 % du contenu est identique.



Kaspersky Hosted Web Security

17 Présentation

- 17.1 Les paramètres de configuration requis pour diriger ce trafic externe via le système Kaspersky Hosted Web Security sont définis et mis à jour par le Client, et dépendent de l'infrastructure technique du Client. Le Client doit faire en sorte que le trafic interne HTTP/FTP sur HTTP (par exemple l'intranet de l'entreprise) ne soit pas dirigé via le KHS. Si le Client a des services Internet exigeant une connexion directe et non via une passerelle par procuration (proxy), il incombe au Client d'opérer les changements nécessaires dans sa propre infrastructure pour que ceci soit possible.
- 17.2 Une fois effectués les changements de configuration appropriés, toutes requêtes d'accès à des pages Web et des pièces jointes sont acheminées par voie électronique via le système Kaspersky Hosted Web Security et examinées numériquement afin d'y détecter tout Logiciel malveillant.
- 17.3 Les requêtes d'accès externe à HTTP et FTP sur HTTP du Client y compris toutes pièces jointes, macros ou exécutable sont dirigées via le système Kaspersky Hosted Web Security. Tout autre contenu acheminé via HTTP (par exemple la lecture en continu (streaming) de contenus multimédia) peut également passer par le système Kaspersky Hosted Web Security, mais sans être scanné.
- 17.4 L'accès au KHS est restreint par l'analyse (scan) des adresses IP, c'est-à-dire l'adresse (ou les adresses) IP dont est issu le trafic Web du Client. L'analyse des adresses IP est également utilisée pour identifier le Client et sélectionner dynamiquement les paramètres spécifiques du Client.
- 17.5 Les utilisateurs peuvent être identifiés d'après l'adresse IP de la passerelle du Client ou via le service d'annuaire.
- 17.6 Kaspersky Hosted Web Security scanne le plus grand nombre possible de pages Web et de leurs pièces jointes. Il peut se produire que certains contenus, pages, et pièces jointes Web soient impossibles à analyser (par exemple en cas de protection par un mot de passe). Les pièces jointes expressément identifiées comme non-analysables (unscannable) ne seront pas bloquées. Le trafic diffusé en continu et crypté (à savoir lors de la lecture continue de contenus multimédia et/ou sur HTTPS/SSL) ne peut être analysé et sera acheminé sans être analysé via le système Kaspersky Hosted Web Security.
- 17.7 Kaspersky Lab insiste sur le fait que la configuration de Kaspersky Hosted Web Security est entièrement sous le contrôle du Client. Le KHS décrit dans la présente Description du KHS est destiné à n'être utilisé que pour permettre au Client d'appliquer une procédure existante, effectivement mise en œuvre, d'utilisation acceptable des ordinateurs (ou équivalente). Dans certains pays, il peut être nécessaire d'obtenir le consentement de chaque membre du personnel, et c'est pourquoi Kaspersky Lab conseille au Client de toujours vérifier sa législation locale avant de déployer Kaspersky Hosted Web Security.
- 17.8 Les e-mails des utilisateurs peuvent être définis par l'administrateur pour les informer de la détection d'un « virus » ou d'un « logiciel espion » (spyware).
- 17.9 L'administrateur peut créer une liste blanche des logiciels publicitaires (adware).

18 Kaspersky Hosted Web Security. Rapports

- 18.1 Des rapports de synthèse peuvent être générés une fois par jour, par semaine, par mois ou par an.
- 18.2 Ces rapports de synthèse peuvent être générés sous forme de graphiques, de tableaux ou en format xml ou csv.
- 18.3 Il est possible de planifier les rapports suivants :
 - 18.3.1 principaux virus bloqués
 - 18.3.2 virus bloqués, par nombre de correspondances
 - 18.3.3 principaux groupes, par virus bloqués
 - 18.3.4 protocoles utilisés, par bande passante
 - 18.3.5 protocoles utilisés, par connexions
 - 18.3.6 principaux utilisateurs, par virus bloqués
 - 18.3.7 indication du trafic autorisé
 - 18.3.8 indication du trafic bloqué
- 18.4 La fréquence des rapports ainsi planifiés peut être :
 - 18.4.1 une fois seulement
 - 18.4.2 une fois par jour
 - 18.4.3 une fois par semaine
 - 18.4.4 une fois par mois
- 18.5 Des rapports peuvent être générés pour des utilisateurs ou des groupes d'utilisateurs particuliers sur une période spécifique.



19 Kaspersky Hosted Web Security. Analyse anti-virus (AV)

- 19.1 Une fois effectués les changements de configuration appropriés, les pages Web et leurs pièces jointes seront analysées par plusieurs moteurs anti-virus.
- 19.2 AV analyse le plus grand nombre possible de pages Web et de leurs pièces jointes. Il peut se produire que certaines pages Web ou certaines pièces jointes soient impossibles à analyser (par exemple en cas de protection par des mots de passe). Les pièces jointes non-analysables seront bloquées. Le trafic crypté (utilisant HTTPS/SSL) ne peut être analysé et sera acheminé via AV sans être analysé.
- 19.3 Si une page Web ou des pièces jointes d'un Client s'avèrent contenir un Logiciel malveillant (ou réputé non-analysable), l'accès à cette page Web ou pièce jointe sera refusé et l'utilisateur d'Internet verra s'afficher une page Web d'alerte automatique de virus. L'administrateur du Client peut également être notifié par e-mail.
- 19.4 AV va analyser les premiers 100 Mb de chaque transfert de fichier. Dans le cas d'un téléchargement de fichiers dépassant 100 Mb, le système analysera les 100 Mb initiaux et le reste sera acheminé directement.

20 Kaspersky Hosted Web Security. Filtrage des logiciels espions (SPS, Spyware Screening)

- 20.1 Une fois effectués les changements de configuration appropriés, le système va analyser et filtrer les pages Web et leurs pièces jointes.
- 20.2 SPS analyse le plus grand nombre possible de pages Web et de leurs pièces jointes. Il peut se produire que certaines pages Web ou certaines pièces jointes soient impossibles à analyser (par exemple en cas de protection par des mots de passe). Les pièces jointes non-analysables seront bloquées. Le trafic crypté (utilisant HTTPS/SSL) ne peut être analysé et sera acheminé via SPS sans être analysé.
- 20.3 Si une page Web ou des pièces jointes d'un Client s'avèrent contenir un logiciel espion (ou réputé non-analysable), l'accès à cette page Web ou pièce jointe sera refusé et l'utilisateur d'Internet verra s'afficher une page Web d'alerte automatique de logiciel espion. L'administrateur du Client peut également être notifié par e-mail.
- 20.4 SPS va analyser les premiers 100 Mb de chaque transfert de fichier. Dans le cas d'un téléchargement de fichiers dépassant 100 Mb, le système analysera les 100 Mb initiaux et le reste sera acheminé directement.

21 Kaspersky Hosted Web Security. Filtrage du Web (WF, Web Filtering)

- 21.1 Une fois effectués les changements de configuration appropriés, le système va filtrer les pages Web et leurs pièces jointes en utilisant une catégorisation des URL et une analyse de contenu. Les URL sont catégorisées d'après un nombre de catégories prédéfinies spécifiées dans le Portail.
- 21.2 Le Client peut configurer WF pour créer des procédures de restriction d'accès (basées à la fois sur la catégorie et sur les types de contenu) et les déployer à des moments spécifiques à l'usage d'utilisateurs ou de groupes d'utilisateurs spécifiques sur Internet. Un certain nombre de fonctions supplémentaires (par exemple la définition des listes d'URL approuvées et bloquées) sont également disponibles.
- 21.3 WF analyse le plus grand nombre possible de pages Web et de leurs pièces jointes. Il peut se produire que certaines pages Web ou certaines pièces jointes soient impossibles à filtrer (par exemple en cas de protection par des mots de passe). Les Clients peuvent également configurer des exceptions spécifiques pour des sites Web ne pouvant être filtrés. Le trafic crypté (utilisant HTTPS/SSL) ne peut être filtré et sera acheminé directement via WF sauf indication contraire par le Client concernant des catégories spécifiques de contenus. WF ne filtrera que les pages Web catégorisées par WF selon la catégorie que le Client a choisi de filtrer.
- 21.4 Le Client a la possibilité d'exercer des fonctions d'administration d'individus et/ou de groupes et de générer des rapports, en utilisant l'Agent logiciel applicatif approprié. L'utilisation de cet Agent sera conditionnée par le Contrat de licence d'utilisateur final fourni avec l'application.
- 21.5 Si un utilisateur d'Internet requiert l'accès à une page Web ou à une pièce jointe à laquelle s'applique une procédure de restriction d'accès, l'accès à cette page Web ou pièce jointe sera refusé et l'utilisateur verra s'afficher une page Web d'alerte automatique. L'administrateur du Client peut également être notifié par e-mail.

22 Kaspersky Hosted Web Security Connector

- 22.1 Kaspersky Lab propose à ses Clients un logiciel nommé « Connector », en option. S'il est commandé par le Client, Kaspersky Lab fournira le logiciel Connector au Client afin qu'il l'installe sur son réseau selon les directives d'installation de Kaspersky Lab. Il existe deux versions de Connector :
 - Workgroup Connector (pour groupes de travail), pour les Clients ayant une configuration réseau simple. Il autorise l'identification d'utilisateurs individuels lors de leur accès aux Services (au moyen d'une licence). Les Clients peuvent ainsi utiliser le Portail pour appliquer des procédures, les administrer et générer des rapports sur des utilisateurs ou groupes définis dans les répertoires existants du Client et pris en charge par le Connector. Workgroup Connector s'exécute de façon autonome et permet le transfert d'e-mails et l'intégration à un Active Directory (AD).



- Enterprise Connector est destiné aux Clients détenant déjà des dispositifs d'accès (ex. ISA Server, Checkpoint, Cisco, Blue Coat) et qui ont besoin de les intégrer au KHS.

22.2 Connector permet aux utilisateurs de se connecter à des Services même sans adresse IP statique, en utilisant une licence. Si les utilisateurs ont d'autres services reposant sur une adresse IP fixe et qu'ils aimeraient voir identifiés, ils peuvent configurer des connexions directes à des sites Web, domaines, hôtes ou réseaux spécifiques.

22.3 Les administrateurs peuvent créer, révoquer, activer et désactiver les licences de ces connexions, par groupe ou par utilisateur.

22.4 Connector ne prend pas en charge tous les systèmes et configurations potentiels du Client. Pour plus d'informations techniques, consultez <http://support.kaspersky.com/faq/?qid=208281752>.

23 Kaspersky Hosted Web Security. Garanties

23.1 Disponibilité. Kaspersky Lab garantit une disponibilité de Kaspersky Hosted Web Security de de 99,999 %.

23.2 La disponibilité de Kaspersky Hosted Web Security se définit comme l'aptitude à recevoir les requêtes sortantes d'accès au Web du Client et ne s'applique que si l'hôte, les dispositifs de passerelle ou la (ou les) passerelle(s) par procuration (proxy) du Client sont correctement configurés pour fonctionner 24 heures sur 24, 7 jours sur 7.

23.3 Toutes les mesures des fonctionnalités et garanties décrites sont définies pour un mois calendaire donné.

23.4 Si Kaspersky Lab ne satisfait pas son engagement de disponibilité défini dans le tableau ci-dessous, le Client peut être en droit de recevoir un avoir selon les pourcentages suivants :

Disponibilité par mois calendaire	Avoir en pourcentage des Frais mensuels
< 99,999 % mais >= 99,99 %	10 %
< 99,99 % mais >= 99 %	25 %
< 99 % mais >= 98 %	50 %
< 98 %	100 %

23.5 Pour recevoir un avoir, le Client doit envoyer une Demande d'avoir à KHS-Support@kaspersky.com dans un délai de 14 (quatorze) jours à compter de la violation de la présente garantie.

