KASPERSKY LAB

Kaspersky® Administration Kit version 5.0

Introduction

KASPERSKY® ADMINISTRATION KIT
VERSION 5.0

Introduction

http://www.kaspersky.com/

Date de révision : Décembre 2005

Sommaire

CHAPITRE 1. INTRODUCTION

Ce document décrit à l'intention d'un administrateur de sécurité les principales étapes à suivre pour mettre en place rapidement et efficacement un système de protection antivirus contenant des applications Kaspersky Lab sur le réseau d'entreprise, en utilisant **Kaspersky Administration Kit**.

Ce document examine un scénario simplifié d'installation de la protection antivirus protection sur plusieurs ordinateurs. Pour réussir l'installation, les ordinateurs doivent être exploités sous Windows NT/2000/2003/XP.

Ce document décrit également la mise à niveau de la version 4.x vers la version 5.x des applications Kaspersky Lab.

Reportez-vous à la documentation complète de Kaspersky Administration Kit pour des informations détaillées sur les fonctions de l'application.

Kaspersky Administration Kit 5 est conçu pour administrer le système de protection antivirus à l'intérieur d'un réseau d'entreprise. Les possibilités offertes par l'application à l'administrateur sont les suivantes :

- Déployer les applications Kaspersky Lab sur le réseau.
- Gérer à distance le système de protection antivirus à partir d'un même poste.
- Recevoir des notifications sur des événements concernant la protection antivirus, à travers le réseau.
- Accumuler des statistiques et des rapports sur toutes les installations.

Kaspersky Administration Kit 5 inclut les composants suivants :

- Le **Serveur d'administration** permet aux administrateurs de gérer de manière centralisée les applications Kaspersky Lab installées sur le réseau. Les applications actuellement prises en charge sont Kaspersky Anti-Virus 5.0 pour stations de travail et Kaspersky Anti-Virus 5.0 pour serveurs de fichiers. Le serveur d'administration conserve toutes les informations sur le système de protection antivirus de l'entreprise dans une base de données Microsoft Development Environment (MSDE) 2000 ou SQL Server 2000. MSDE 2000 Service Patch (SP) 3 ou MS SQL

Server 2000 SP 3 doivent avoir été installés et configurés avant l'installation du serveur d'administration. Vous pouvez installer MSDE 2000 SP 3 à partir du paquet inclus dans le kit de distribution de Kaspersky Administration Kit 5.

- L'**Agent réseau** (Network Agent) est installé sur des postes de travail protégés par Kaspersky Anti-Virus 5.0 pour stations de travail ou pour serveurs de fichiers, et contrôlé par l'intermédiaire du serveur d'administration. Ce composant coordonne l'interaction entre les applications Kaspersky Lab exécutées sur les postes clients, et le serveur d'administration. L'agent réseau reçoit des ordres du serveur d'administration et transmet des renseignements sur la protection antivirus des postes clients.

- La **Console d'administration** fournit l'interface utilisateur nécessaire pour les services d'administration du serveur et de l'agent. Ce composant s'intègre dans Microsoft Management Console (MMC).

CHAPITRE 2. PREMIERS PAS

Pour créer un périmètre de protection efficace autour de votre réseau d'entreprise, suivez ces étapes:

1. Installez MSDE 2000 SP 3 ou SQL Server 2000 SP 3 (voir section 2.1 à la page 7). Passez cette étape si votre réseau possède une installation de l'un ou l'autre de ces serveurs de base de données.

2. Installez le serveur d'administration, et la console d'administration (voir section .2.2 à la page 8).

3. Faites une première configuration du système de protection antivirus à l'aide de l'Assistant Démarrage rapide (voir section 2.3 à la page 9).

4. Créez les groupes d'administration afin de contrôler des groupes de postes clients, par l'application de stratégies et des tâche de groupe (voir section 0 à la page 11).

5. Installez à distance l'agent réseau sur les postes clients pour que leurs applications antivirus puissent réagir au serveur d'administration (voir section 2.5 à la page 11).

6. Installez à distance Kaspersky Antivirus 5 pour Stations de travail ou pour Serveurs de fichiers sur les postes clients sélectionnés (voir section .2.6 à la page 12).

7. Configurez le téléchargement des mises à jour des bases antivirus par Internet par le serveur d'administration, puis vérifiez que l'opération se réalise correctement. Vérifiez la mise à jour des bases de données sur les postes clients (voir section 2.7 à la page 13).

8. Configurez les notifications à l'administrateur sur les événements liés aux virus sur les postes clients (voir section 2.8 à la page 14).

9. Sur les postes clients, lancez une analyse à la demande et vérifiez que la tâche de notification est exécutée (voir section 2.9 à la page 15).

10. Affichez un compte-rendu de protection antivirus portant sur les postes clients, et sur le nombre de virus détectés par les applications Kaspersky Lab (voir section 2.10 à la page 16).

Si les étapes précédentes se sont déroulées avec succès, cela signifie que vous avez établi un système de protection antivirus fiable pour votre réseau.

Les sections suivantes décrivent ces étapes de manière plus détaillée.

2.1. Installation de MSDE

Passez cette étape si votre réseau est déjà équipé de Microsoft Development Environment (MSDE) 2000 SP 3 ou de SQL Server 2000 SP 3.

Pour installer MSDE 2000 depuis le paquet d'installation de Kaspersky Administration Kit,

1. Sélectionnez l'ordinateur où vous allez installer la base de données du serveur d'administration. Normalement, il s'agit du même ordinateur sur lequel est installé le serveur d'administration.

2. Exécutez le fichier **setup.exe** dans le répertoire **MSDE2KSP3** du CD d'installation de Kaspersky Administration Kit 5.0.

3. Suivez les instructions de l'Assistant d'installation.

Après avoir effectué toutes les étapes, l'application MSDE 2000 SP 3 sera installée sur le poste sélectionné. MSDE 2000 SP 3 n'exige aucune administration.

La version de MSDE présente dans le paquet de Kaspersky Administration Kit ne peut être utilisée qu'avec Kaspersky Administration Kit.

Le serveur d'administration conserve toutes les informations sur le système de protection antivirus de l'entreprise dans une base de données Microsoft Development Environment (MSDE) 2000 SP3 ou SQL Server 2000 SP3.

L'application **klbackup** présente dans le paquet de distribution de Kaspersky Administration Kit fera des sauvegardes des données du serveur d'administration. Pour plus de détails sur cet outil, reportez-vous au Guide de l'administrateur.

2.2. Installation du serveur d'administration et de la console d'administration

Pendant l'installation, Vous avez le choix entre l'installation du serveur d'administration avec la console d'administration, ou seulement de la console d'administration. Vous ne pouvez pas installer le serveur d'administration sans la console. L'option par défaut installe les deux composants.

Si nécessaire, vous pouvez installer la console d'administration sur un autre ordinateur, et gérer le serveur d'administration depuis le réseau.

Pour installer le serveur d'administration et/ou la console d'administration,

1. Sélectionnez l'ordinateur où vous allez installer les composants. S'il votre réseau utilise une structure de domaine Windows, il est recommandé d'installer le serveur d'administration sur un membre du domaine.

   Vous pouvez installer la version 5.x de Administration Server sur le même ordinateur utilisé pour la version 4.x. Les serveurs d'administration des versions 5.x et 4.x sont indépendants les uns des autres et peuvent ктre exploités côte a côte, sur un mкme ordinateur, sans poser de problèmes de compatibilité.

   Il est conseillé de posséder des droits d'administrateur du domaine pour installer le produit. Ceci permet de créer automatiquement les groupes **KLAdmins** et **KLOperators**, et d'accorder les crédits nécessaires au compte utilisé par le serveur d'administration pour opérer.

2. Lancez le programme setup.exe à partir du CD d'installation de Kaspersky Administration Kit 5.

3. Suivez les instructions de l'Assistant.

   Utilisez le compte de l'administrateur de domaine comme compte de service utilisé pour démarrer le serveur d'administration.

2.3. Assistant Démarrage rapide

Pour effectuer la configuration initiale de la protection antivirus ,

1. Lancez la console d'administration : cliquez sur **Démarrer→ Programmes → Kaspersky Administration Kit → Kaspersky Administration Kit**.

2. Connectez-vous au serveur d'administration cible : cliquez sur l'entrée Serveur d'administration dans l'arborescence de console. Acceptez le certificat du serveur.

3. Dans le menu contextuel, cliquez sur **Assistant Démarrage rapide**.

4. Attendez jusqu'à ce que le serveur d'administration termine l'exploration du réseau et détecte tous les ordinateurs.

5. Créez des groupes d'administration par l'une des méthodes suivantes :

   - Puisque nous procédons uniquement avec quelques ordinateurs de test, cliquez sur **Manuellement** et ajoutez manuellement des postes clients à ce groupe.

   - Si vous êtes en train de déployer le système de protection antivirus à travers un réseau corporatif, l'une des méthodes suivantes vous permet de créer automatiquement les réseaux logiques :

     - **Ajouter des postes au groupe à partir du réseau de Windows**. Dans ce cas, le réseau logique utilisera une structure semblable à celle des domaines et des groupes d'utilisateurs du réseau Windows (les groupes d'administration coïncideront avec les domaines Windows et les groupes d'utilisateur).

     - **Ajouter des postes au groupe selon la structure de la version précédente de Kaspersky Administration Kit**. Dans ce cas, le réseau logique sera semblable à celui de Kaspersky Administration Kit 4.x.

6. Sélectionnez les options permettant d'envoyer des courriers de notification générés par les applications Kaspersky Lab. Ces paramètres

sont modifiables dans les propriétés du serveur d'administration. Pour plus d'informations, reportez-vous au Guide de l'administrateur.

7. Créez une stratégie pour Kaspersky Antivirus 5 pour Stations de travail, et définissez plusieurs tâches afin d'activer le système de protection antivirus. Kaspersky Administration Kit 5 fait appel à des stratégies de groupe pour appliquer uniformément la même configuration à tous les ordinateurs d'un groupe. Les tâches sont des actions effectuées par le logiciel antivirus sur tous les ordinateurs du groupe.

   L'Assistant créera les stratégies et les tâches suivantes:

   - Une stratégie de haut niveau pour toutes les applications antivirus, avec une configuration par défaut. Par la suite, vous pourrez afficher et modifier les paramètres de stratégie. Pour appliquer les modifications de stratégie dans les postes clients, et pour éviter que l'utilisateur puisse les modifier à son tour, utilisez l'icône  .

   - Une tâche globale pour la mise à jour du serveur d'administration par Internet.

     L'application téléchargera les mises à jour, à la fois des bases antivirus et des modules de programme, à partir d'un serveur de mises à jour de Kaspersky Lab et les enregistrera dans le dossier partagé spécifié lors de l'installation du serveur d'administration. Les postes clients récupèreront leurs mises à jour à travers ce dossier partagé. Cliquez sur **Paramètres de mise à jour** pour configurer les options de mise à jour du serveur d'administration.

   - Une tâche de haut niveau pour la mise à jour des bases antivirus sur les postes clients sera créée sur les postes clients, avec des valeurs par défaut. Les postes clients seront programmés pour récupérer les mises dans le dossier partagé.

   - Une tâche d'analyse à la demande des postes clients sera créée avec des valeurs par défaut.

2.4. Création d'un groupe d'administration

Pour ajouter un nouveau groupe au réseau logique,

1. Dans l'arborescence de console ou dans le dossier **Groupes** du panneau de détails, sélectionnez un groupe auquel vous allez ajouter un nouveau groupe. Ouvrez le menu contextuel et cliquez sur **Nouveau → Groupe** pour lancer un Assistant Nouveau groupe. Suivez les instructions de l'Assistant.

2. Déplacez les postes sélectionnés du groupe **Réseau** vers le nouveau groupe : vous pouvez utiliser un copier-coller ou un glisser-déplacer.

   Si une installation de Kaspersky Lab Anti-Virus 4.x existe déjà sur les postes clients sélectionnés, elle sera écrasée automatiquement pendant l'installation distante de la version 5.x.

2.5. Installation distante de l'agent réseau

Pour installer Network Agent à partir d'un emplacement distant,

1. Lancez l'Assistant de déploiement d'application dans le menu contextuel de la console d'administration.

2. Sélectionnez le paquet d'installation de Network Agent créé par l'Assistant Démarrage rapide. Ce paquet est créé au cours de l'installation du serveur d'administration et contient les paramètres utilisés par l'agent réseau pour se connecter au serveur d'administration.

3. Définissez le groupe d'administration contenant les postes cibles sur lesquels installer Network Agent.

Si le compte de service du serveur d'administration ne possède pas de privilèges d'administrateur sur les postes clients sélectionnés, saisissez l'utilisateur et le mot de passe administrateurs de ces postes clients.

4. La tâche d'installation à distance démarre alors. À la fin de la tâche, l'agent réseau aura été installé sur les ordinateurs clients spécifiés. Dans la boîte de dialogue suivante de l'Assistant, vous pouvez voir la progression de la tâche d'installation à distance et l'historique des tâches de chacun des postes clients.

5. À la fin de la tâche, examinez les résultats et quittez l'Assistant de déploiement d'application.

6. Si vous souhaitez gérer la protection antivirus du poste client en temps réel, et pour être sûr que le serveur d'administration peut se connecter à l'agent réseau à tout moment, il faut que le port numéro 15000 soit ouvert sur le poste client. Si le port UPD ne peut pas être ouvert, cochez la case **Maintenir la connexion** sur l'onglet **General** de la boîte de dialogue **Propriétés : <nom du poste>** utilisé pour configurer les paramètres du poste client.

Pour vérifier que l'installation est réussie, cliquez sur **Propriétés** dans le menu contextuel de l'un des postes sur lequel vous venez d'installer l'agent réseau. Vérifiez que l'application Kaspersky Network Agent est signalée en **Exécution** dans l'onglet **Applications**.

Si le déploiement réussi mais l'agent réseau n'est pas en mesure de se connecter au serveur d'administration, utilisez l'outil kinagchik.exe. Cet outil est fourni avec le paquet de distribution de Network Agent et se trouve à la racine du dossier d'installation de l'agent réseau après son installation. Depuis la ligne de commande, cet outil réalise un diagnostic détaillé de la configuration de la connexion du serveur d'administration.

2.6. Déploiement de l'application Kaspersky Anti-Virus

Cette section se concentre sur l'installation décentralisée de Kaspersky Anti-Virus for Windows Workstation. La procédure de déploiement d'autres applications Kaspersky Lab est semblable à celle décrite ci-après.

Pour déployer à distance Kaspersky Anti-Virus for Windows Workstation sur des postes réseau,

1. Créez un paquet d'installation pour Kaspersky Antivirus 5 pour Stations de travail à l'aide d'un Assistant. L'Assistant peut être démarré à l'aide de la commande **Installation à distance** du menu contextuel.

   Le fichier **.kpd** requis pour créer le paquet d'installation se trouve dans la racine du fichier de distribution de Kaspersky Antivirus 5 pour Stations de travail. Le fichier-clé de licence pour Kaspersky Antivirus 5 pour Stations de travail se trouve également dans ce répertoire racine.

   Si nécessaire, configurez le paquet d'installation. Il est recommandé, par exemple, d'autoriser le redémarrage automatique des postes clients.

2. Lancez l'Assistant de déploiement d'application, dans le menu contextuel du serveur d'administration.

3. Installez Kaspersky Antivirus 5 pour Stations de travail à partir du paquet, comme vous avez fait pour installer Network Agent (voir section 2.5 à la page 11). Vous pouvez également installer l'agent réseau en même temps que Kaspersky Anti-Virus for Windows Workstation.

   Vous pouvez installer Kaspersky Anti-Virus 5.x sur des ordinateurs équipés d'applications de la version 4.x. Dans ce cas, les applications de la version 4.x seront automatiquement écrasées par ceux de la version 5.x.

Pour vérifier que l'installation s'est faite correctement, choisissez l'un des postes clients sur lequel vous venez d'installer l'application, et ouvrez sa fenêtre de propriétés. Ouvrez l'onglet **Applications** et vérifiez que l'application Kaspersky Anti-Virus pour stations de travail 5 application est signalée en **Exécution**. L'onglet **Tâches** doit afficher la tâche de protection en temps réel exécutée par Kaspersky Antivirus 5 pour Stations de travail.

2.7. Vérification de l'exécution de la tâche de mise à jour

Pour vérifier que les postes clients récupèrent correctement les mises à jour,

1. Exécutez la tâche de mise à jour sur le serveur d'administration, dans le niveau supérieur de l'entrée **Tâche** de l'arborescence de console. L'Assistant Démarrage rapide crée automatiquement cette tâche. L'application téléchargera les mises à jour à partir d'un serveur de mises à jour de Kaspersky Lab et les enregistrera dans le dossier partagé spécifié lors de l'installation du serveur d'administration. Patientez jusqu'à ce que la tâche soit terminée.

   Cliquez sur **Historique** pour voir la réponse en sortie de la tâche.

   Pour voir la liste de mises à jour téléchargées, cliquez sur l'entrée **Mises à jour** dans l'arborescence de console.

   

   Des détails sur la procédure de mise à jour sont disponibles sur le site Web de Kaspersky Lab (http://www.kaspersky.ru/avupdates).

2. Lancez la tâche de mise à jour de groupe sur les postes clients. Cette tâche est créée par l'Assistant Démarrage rapide, et conservée dans le dossier **Tâches** de l'entrée **Groupe**. Patientez jusqu'à ce que la tâche soit terminée.

   Cliquez sur **Historique** pour voir la réponse en sortie de la tâche.

La tâche créée par l'Assistant Démarrage rapide met à jour les postes clients à travers la connexion entre l'agent réseau et le serveur d'administration. Les méthodes suivantes de mise à jour des postes clients sont également prises en charge :

- Dans le dossier partagé du serveur d'administration ;
- Par un serveur HTTP ;
- Par un serveur FTP.

Pour pouvoir copier les dernières mises à jour depuis le dossier partagé, les postes clients doivent posséder des privilèges de lecture sur ce dossier. Si, pour une raison ou une autre, ceci est impossible, utilisez un serveur FTP ou HTTP pour déployer les mises à jour sur les postes clients. Créez un répertoire FTP ou HTTP associé au sous-dossier **Mises à jour**, du dossier partagé, dans lequel le serveur d'administration enregistrera les mises à jour téléchargées par Internet (par exemple, ftp://admserver/updates). Spécifiez ce dossier (ftp://admserver/updates) en tant que source des tâches de mise à jour exécutées sur les postes clients.

2.8. Configuration des notifications

Pour recevoir des notifications d'événements liés à la protection antivirus,

1. Ouvrez l'onglet **Traitement des événements** dans les Propriétés de la stratégie de haut niveau d'une application antivirus (par exemple, Kaspersky Anti-Virus pour stations de travail).

2. Sur cet onglet, spécifiez les événements sur lesquels vous souhaitez être informé et précisez comment les notifications vous seront envoyées.

   Pour tester le système de notifications (voir section 2.9 à la page 15), il suffit de configurer une notification d'événement **Virus détecté**.

3. L'icône  pour tous les paramètre configurés, afin de les étendre à tous les postes clients. Pour appliquer les modifications, appuyez sur **Appliquer**.

4. Vous pouvez vérifier votre configuration par l'envoi manuel d'un message. Pour ce faire, cliquez sur **Test**. Les messages créés d'après le modèle spécifié seront envoyés aux adresses indiquées dans les paramètres.

2.9. Mise à l'essai du système de notifications et de la tâche d'analyse à la demande

Pour tester le système de notifications et la tâche d'analyse à la demande,

1. Essayez de copier le virus de test **Eicar** vers l'ordinateur protégé. L'opération de copie échouera si la tâche de protection en temps réel est en cours d'exécution. Vous devez recevoir une notification sur la détection d'un virus, et cet événement doit être enregistré sous l'entrée **Événements** dans l'arborescence de console.

   

   Le « virus d'essai » EICAR n'est pas un vrai virus et il ne contient aucun code qui puisse nuire à votre ordinateur. Néanmoins, la majorité des logiciels antivirus identifient ce fichier comme un virus. Vous pouvez télécharger le « virus d'essai » sur le site officiel de l'organisation **EICAR** à l'adresse http://www.eicar.org/anti_virus_test_file.htm.

2. Arrêtez la tâche de protection en temps réel sur le poste client. Copiez le virus d'essai **Eicar** sur le poste client et activez à nouveau la tâche de protection en temps réel.

3. Lancez la tâche de groupe d'analyse à la demande sur un groupe de postes clients. Comme résultat, l'application doit détecter le fichier eicar.com et vous envoyer une notification à son sujet. Un enregistrement sur cet événement doit apparaître sous l'entrée **Événements** de l'arborescence de console.

2.10. Génération de rapports

Le programme peut générer des rapports sur l'état actuel du système de protection antivirus à partir du journal d'événements de Kaspersky Administration Kit, conservé sur le serveur d'administration. Les modèles de rapport sont conservés sont disponibles dans l'entrée **Rapports** de l'arborescence de console.

Il existe sept modèles standard qui correspondent à autant de types de rapports :

- **Rapport de version des bases antivirus**
- **Rapport d'erreurs**
- **Rapport sur les licences**
- **Rapport sur les postes les plus infectés**
- **Rapport de protection**
- **Rapport de version du logiciel**
- **Rapport d'activité antivirus**

Par exemple, un rapport d'activité antivirus créé à l'aide du modèle correspondant contiendra des informations sur toutes les apparitions de virus enregistrées par Kaspersky Administration Kit.

Si vous ajoutez au groupe d'administration un ordinateur non équipé de l'agent réseau, le rapport de protection indiquera que ce poste n'est pas protégé.

CHAPITRE 3. MISE A NIVEAU DE LA VERSION 4.X A LA VERSION 5.X

Cette section décrit la mise a niveau des applications Kaspersky Lab version 4.x vers Kaspersky Antivirus pour Stations de travail version 5.x, ou vers Kaspersky Antivirus pour Serveur de fichiers version 5.x. Certaines de ces étapes ont été décrites précédemment. Les instructions suivantes vous permettront de réaliser pas a pas une transition sans difficultés.

Kaspersky Administration Kit 5.x est indépendant de Kaspersky Administration Kit 4.x dans son fonctionnement. Le système d'administration de la version 5.x ne contrôle que des applications de la version 5.x, et réciproquement. Par conséquent, pendant la transition, il est possible de faire fonctionner deux systèmes d'administration côte a côte sur les postes connectés au réseau.

Voici un scénario de transition typique :

1. Installez le serveur d'administration de la version 5.x. Vous pouvez l'installer sur le mкme ordinateur que celui de la version 4.x.

2. Créez une structure de réseau logique de groupes d'administration pour les applications de la version 5.x. Cette structure peut кtre importée du système d'administration de la version 4.x.

3. Créez des stratégies et des tвches de groupe pour les applications de la version 5.x sur le réseau logique. Configurez les paramètres nécessaires et définissez des règles de traitement des événements, liés a la protection antivirus.

4. Spécifiez quels postes vont basculer de la version 4.x a la version 5.x.

5. Créez un paquet d'installation pour les applications de la version 5.x, puis installez les applications de la version 5.x sur les ordinateurs choisis. Pendant l'installation, les applications de la version 4.x sont automatiquement écrasées par les applications de la version 5.x.

6. Les postes équipés du logiciel antivirus de la version 5.x sont ajoutés au réseau logique de la version 5.x du serveur d'administration. Les

ordinateurs restants resteront sous le contrôle du système d'administration de la version 4.x.

De cette manière, l'environnement système de protection antivirus de votre entreprise, encore basé sur la version précédente, fera graduellement la transition vers les applications et le système d'administration de la version 5.x.

CHAPITRE 4. CONCLUSION

Kaspersky Administration Kit 5 dispose d'une panoplie de composants administratifs, qui vont bien plus loin que ceux décrits dans ce document. Ce document décrit les principes de base nécessaires pour bien démarrer avec Kaspersky Administration Kit 5 et pour déployer le système de protection antivirus sur plusieurs ordinateurs connectés au réseau. Ce scénario simplifié montre comment résoudre les problèmes de base liés à l'établissement d'un système de protection fiable, permettant à l'administrateur de :

- Déployer et configurer l'administration du système de protection antivirus
- Déployer des applications antivirus sur plusieurs postes clients à partir d'un même poste centralisé.
- Définir la stratégie de protection antivirus
- Créer et examiner le fonctionnement de la tâche de mise à jour sur les postes clients
- Tester le fonctionnement de la tâche de protection en temps réel.
- Créer et examiner la tâche d'analyse à la demande sur les postes clients
- Définir des règles pour l'envoi de notifications an cas d'événements critiques.
- Produire et afficher des rapports sur le système de protection antivirus

ANNEXE A. KASPERSKY LAB

Fondé en 1997, Kaspersky Lab est devenu un leader reconnu en technologies de sécurité de l'information. Il produit un large éventail de logiciels de sécurité des données, et distribue des solutions techniquement avancées et complètes afin de protéger les ordinateurs et les réseaux contre tous types de programmes malveillants, les courriers électroniques non sollicités ou indésirables, et contre les tentatives d'intrusion.

Kaspersky Lab est une compagnie internationale. Son siège principal se trouve dans la Fédération Russe, et la société possède des délégations au Royaume Uni, en France, en Allemagne, au Japon, aux États-Unis (Canada), dans les pays du Bénélux, en Chine et en Pologne. Un nouveau service de la compagnie, le centre européen de recherches anti-Virus, a été récemment installé en France. Le réseau de partenaires de Kaspersky Lab compte plus de 500 entreprises du monde entier.

Aujourd'hui, Kaspersky Lab emploie plus de 250 spécialistes, tous spécialistes des technologies antivirus : 9 d'entre eux possèdent un M.B.A, 15 autres un doctorat, et deux experts siègent en tant que membres de l'organisation pour la recherche antivirus en informatique (CARO).

Kaspersky Lab offre les meilleures solutions de sécurité, appuyées par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus d'ordinateur. Une analyse complète du comportement des virus d'ordinateur permet à la société de fournir une protection complète contre les risques actuels, et même contre les menaces futures. La résistance à de futures attaques est la stratégie de base mise en œuvre dans toutes les applications Kaspersky Lab. Les produits de la société ont toujours fait preuve d'une longueur d'avance sur ceux de ses nombreux concurrents, pour améliorer la protection antivirus aussi bien des utilisateurs domestiques que des entreprises clientes.

Des années de dur travail ont fait de notre société l'un des leaders de la fabrication de logiciels de sécurité. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Le produit vitrine de la société est Kaspersky Antivirus : il assure une protection complète de tous les périmètres réseau, et couvre les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. Ses outils de gestion intuitifs et faciles à utiliser se prêtent à une automation avancée, en vue d'une protection antivirus rapide à l'échelle de l'entreprise. De nombreux fabricants reconnus utilisent le noyau Kaspersky Antivirus : Nokia ICG (États-Unis), F-Secure (Finlande), Aladdin (Israël), Sybari (États-Unis), G Data (Allemagne),

Deerfield (États-Unis), Alt-N (États-Unis), Microworld (Inde), BorderWare (Canada), etc.

Les clients de Kaspersky Lab profitent d'un large éventail de services supplémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. La base antivirus de Kaspersky Lab est mise à jour en temps réel toutes les 3 heures. La société offre à ses clients un service technique 24/24, disponible en plusieurs langues, et adapté à une clientèle internationale.

A.1. Autres produits antivirus

Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus® Personal protège les ordinateurs personnels tournant sous Windows 98/ME, 2000/NT/XP contre tous les types de virus connus, y compris les logiciels à risque (riskware). Le programme contrôle en permanence toute les sources d'infection potentielles : le courrier électronique, Internet, les disquettes, les CD-Rom, etc. Le système unique d'analyse heuristique des données neutralise efficacement les virus inconnus. Le logiciel peut fonctionner dans l'un des modes suivants (ces différents modes peuvent être utilisés séparément ou conjointement) :

- La **protection en temps réel** permet de rechercher la présence éventuelle de virus dans tous les objets exécutés, ouverts et enregistrés sur l'ordinateur.

- **L'analyse à la demande** permet de rechercher la présence éventuelle de virus et de réparer, le cas échéant, les objets infectés sur tout l'ordinateur ou sur des disques, dans des fichiers ou des dossiers particuliers. Cette analyse peut-être lancée manuellement ou automatiquement selon un horaire défini.

Kaspersky Anti-Virus®Personal ignore à chaque analyse les objets qui n'ont pas été modifiés depuis la dernière analyse, aussi bien dans le cadre de l'analyse en temps réel qu'à la demande. Ceci se traduit par une **nette augmentation de la rapidité d'exécution de l'application**.

Le logiciel représente donc un obstacle de taille pour les virus qui tenteraient d'infecter l'ordinateur via le courrier électronique. Kaspersky Anti-Virus® Personal analyse et répare automatiquement tous les messages entrants et sortants via

les protocoles POP3 et SMTP. Il décèle également avec efficacité les virus dans les bases de données de messagerie.

Le logiciel est compatible avec plus de 700 formats de fichiers archivés ou compressés et assure l'analyse antivirale automatique de leur contenu. Il peut également supprimer tout code malveillant des fichiers archivés au format **ZIP, CAB, RAR, ARJ**.

La simplicité de la configuration du logiciel est assurée grâce à l'existance de trois niveaux prédéfinis : **Sécurité maximale**, **Recommandé** et **Vitesse maximale**.

Les bases de données antivirus sont actualisées toutes les trois heures. Leur distribution est garantie même en cas de coupure ou de modification de la connexion.

Kaspersky Anti-Virus® Personal Pro

Le paquet logiciel est conçu pour offrir une protection antivirale intégrale des ordinateurs personnels sous système d'exploitation Windows 98/ME, Windows 2000/NT, et Windows XP, ainsi que des applications MS Office. Kaspersky Anti-Virus® Personal Pro dispose d'un outil intégré de mise à jour pour le téléchargement des bases de données antivirus et des modules de programmes. Un système exclusif d'analyse heuristique détecte efficacement même les virus inconnus. Ce système d'analyse heuristique de seconde génération parvient à neutraliser les virus inconnus. L'utilisateur peut facilement configurer l'application à travers une interface simple et facile.

Kaspersky Anti-Virus® Personal Pro possède les caractéristiques suivantes :

- **Analyse à la demande** des unités locales ;
- **Protection automatique en temps réel** de tous les fichiers, contre les virus;
- **Filtre de courrier** qui analyse et désinfecte automatiquement tout le trafic de messagerie entrant et sortant de n'importe quel client de messagerie utilisant les protocoles POP3 et SMTP et détecte efficacement les virus dans les bases de données de messagerie ;
- **Bloqueur de comportements** qui assure une protection maximale des applications MS Office contre les virus ;

- **Analyseur de fichier compressés –** Kaspersky Anti-Virus prend en charge plus de 700 formats de fichiers d'archives ou compressés ; il assure l'analyse antivirale automatique de leur contenu, ainsi que la suppression de tout code dangereux dans les fichiers au format **ZIP**, **CAB**, **RAR** ou **ARJ**.

Kaspersky® Anti-Hacker

Kaspersky® Anti-Hacker est un pare-feu personnel destiné à la protection d'un ordinateur sous système d'exploitation Windows. Il le protège contre l'accès non autorisé aux données contenues et contre les attaques extérieures d'intrus provenant d'un réseau local adjacent et d'Internet.

Kaspersky® Anti-Hacker surveille l'activité réseau sous protocole TCP/IP de toutes les applications fonctionnant sur votre machine. Le logiciel détecte n'importe quelle action d'une application suspecte et bloque son accès au réseau. Cette solution permet de protéger vos données confidentielles sur votre machine.

La technologie SmartStealth™ rend la détection de votre ordinateur depuis l'extérieur très difficile: en étant invisible, votre ordinateur est protégé contre les attaques des pirates informatiques et cela n'a absolument aucune influence négative sur votre utilisation d'Internet. Le logiciel garantit la transparence et l'accès normal aux données.

Kaspersky® Anti-Hacker bloque les attaques réseau malicieuses les plus fréquentes et est à l'affût des tentatives d'analyse des ports de votre ordinateur.

Le logiciel permet une administration simplifiée, avec un choix de cinq niveaux de sécurité. Par défaut, le logiciel démarre en mode apprentissage, qui configure automatiquement la sécurité de votre système en fonction de vos réponses à des événements variés. Ce mode permet de configurer le pare-feu pour un utilisateur et un ordinateur particulier.

Kaspersky® Personal Security Suite

Kaspersky® Personal Security Suite est une suite logicielle conçue pour organiser la protection intégrée des ordinateurs personnels tournant sous Windows. Cette solution bloque l'intrusion des programmes malveillants et des riskwares via toutes les sources d'infection possible, vous protège contre l'accès non-autorisés à vos données et lutte contre le courrier indésirable

Kaspersky® Personal Security Suite possède les fonctions suivantes :

- Protection des données de votre ordinateur contre les virus.

- Protection des utilisateurs des clients de messagerie Microsoft Outlook et Microsoft Outlook Express contre le courrier indésirable.

- Protection de l'ordinateur contre l'accès non-autorisé aux données ainsi que contre les attaques de pirates informatiques réalisées depuis le réseau local ou Internet.

Kaspersky® Security for PDA

Le logiciel Kaspersky® Security for PDA protège de manière fiable les données enregistrées sur vos appareils nomades de différents types et sur vos téléphones intelligents. Le logiciel contient un bouquet d'outils antivirus bien ciblés :

- **Un scanner antivirus** qui analyse, à la demande de l'utilisateur, les informations enregistrées aussi bien dans la mémoire du PDA ou du téléphone intelligent que sur n'importe quel type de carte mémoire ;

- **Un moniteur antivirus** qui intercepte les virus au cours de la synchronisation à l'aide de la technologie HotSync™ vers d'autres périphériques.

Kaspersky® Security for PDA est également conçu pour protéger les données stockées dans les ordinateurs de poche (les PDA) contre les accès non autorisés grâce au chiffrement de l'accès à l'appareil et à l'ensemble des données sauvegardées des ordinateurs portables ou des cartes mémoire.

Kaspersky Anti-Virus® Business Optimal

Ce paquet logiciel offre une protection intégrale des données sur des réseaux des petites et moyennes entreprises.

Kaspersky Anti-Virus® Business Optimal offre une protection antivirale[1] intégrale de :

- Postes de travail sous Windows 98/ME, Windows NT/2000/XP Workstation et Linux ;

[1] En fonction du type de livraison

- *Serveurs de fichiers* sous Windows NT 4.0 Server, Windows 2000/2003 Server/Advanced Server, Novell Netware, FreeBSD et OpenBSD, Linux et Samba Servers ;

- *Système de messagerie* Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail et Qmail ;

- *Passerelle-Internet* : CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition.

Kaspersky Anti-Virus® Business Optimal comprend également un système d'installation et d'administration centralisé : le Kaspersky® Administration Kit.

Vous pouvez choisir librement les logiciels antivirus en fonction du système d'exploitation et des applications que vous utilisez.

Kaspersky® Corporate Suite

Ce paquet logiciel offre une protection intégrale des données sur des réseaux de toutes dimensions et de tous degrés de complexité. Les composants du paquet logiciel assurent la protection de tous les postes d'un réseau d'entreprise. Compatibles avec la majorité des systèmes d'exploitation et des applications utilisés actuellement, les composants sont unis par un système d'administration centralisé et disposent d'une interface utilisateur identique. La flexibilité de cette solution antivirus permet de créer un système de protection efficace prenant en charge de manière parfaitement appropriée toutes les configurations de votre réseau.

Kaspersky® Corporate Suite garantit la protection antivirale intégrale de :

- *Postes de travail* sous Windows 98/ME, Windows NT/2000/XP Workstation et Linux ;

- *Serveurs de fichiers* sous Windows NT 4.0 Server, Windows 2000/2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD, Linux et Samba Servers ;

- *Système de messagerie* Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail et Qmail ;

- *Passerelle-Internet* : CheckPoint Firewall –1; Microsoft ISA Server 2004 Enterprise Edition ;

- *Ordinateurs de poche* sous Windows CE et Palm OS et téléphones intelligents tournant sous Windows Mobile 2003 for Smartphone et Microsoft Smartphone 2002.

Kaspersky® Corporate Suite dispose également d'un *système d'installation et d'administration centralisé* : Kaspersky® Administration Kit.

Vous pouvez choisir librement les logiciels antivirus en fonction du système d'exploitation et des applications que vous utilisez.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam est une suite logicielle performante conçue pour protéger les réseaux des petites et moyennes entreprises contre les courriers électroniques non désirés (spam). Ce produit combine les techniques révolutionnaires d'analyse linguistique des messages, avec l'ensemble des méthodes de filtrage de courrier électronique modernes (y compris les listes noires, ou listes RBL). Il inclut une collection unique de services permettant aux utilisateurs d'identifier et de nettoyer près de 95% du trafic non souhaité.

Kaspersky® Anti-Spam se comporte comme un filtre, placé à l'entrée du réseau, qui analyse les flux entrants de courrier électronique à la recherche d'objets identifiés en tant que courrier indésirable. Le logiciel est compatible avec tous les systèmes de messagerie existants sur votre réseau et il peut être installé aussi bien sur un serveur de messagerie existant ou sur un serveur dédié.

Les hautes performances de Kaspersky® Anti-Spam sont possibles grâce à des mises à jour quotidiennes des bases de données utilisées par les filtres, à partir des échantillons fournis par les spécialistes linguistiques du laboratoire.

Kaspersky SMTP Gateway

Kaspersky® SMTP-Gateway for Linux/Unix est une solution conçue pour le traitement antivirus des messages livrés via le protocole SMTP. L'application contient toute une série d'outils de filtrage du flux de messagerie : selon le nom et le type MIME des fichiers joints ainsi que plusieurs moyens permettant de réduire la charge du système de messagerie et de prévenir les attaques de pirates informatiques. Citons, entre autres, les restrictions au niveau de la taille des messages, du nombre de destinataires, etc. La prise en charge de la technologie DNS Black List évite de recevoir des messages en provenance de serveurs repris dans la liste des serveurs de diffusion de courrier indésirable.

Kaspersky Security® for Microsoft Exchange 2003

Kaspersky Security for Microsoft Exchange recherche la présence éventuelle de virus dans le courrier entrant et sortant, ainsi que dans les messages enregistrés sur le serveur, y compris les messages dans les dossiers partagés. Il rejette également le courrier indésirable grâce à l'exploitation de technologies intelligentes d'identification des messages non sollicités conjointement aux technologies développées par Microsoft. L'application recherche la présence d'éventuels virus dans tous les messages qui arrivent sur le serveur Exchange via le protocole SMTP à l'aide de technologies mises au point par Kaspersky Lab et identifie le courrier indésirable grâce à des filtres formels (adresse électronique, adresse IP, taille du message, en-tête) et à l'analyse du contenu du message et des pièces jointes à l' aide de technologies intelligentes dont des signatures graphiques uniques qui permettent d'identifier le courrier indésirable sous forme graphique. Le corps du message et les pièces jointes sont soumis à l'analyse.

Kaspersky® Mail Gateway

Kaspersky Mail Gateway est une solution universelle pour la protection avancée des utilisateurs des systèmes de messagerie. L'application, qui est installée entre le pare-feu de l'entreprise et Internet, analyse tous les éléments du message électronique et recherche la présence éventuelle de virus et d'autres programmes malveillants (spyware, adware, etc.). Il opère également un filtrage centralisé du courrier afin d'identifier le courrier indésirable. Le logiciel offre aussi plusieurs autres possibilités en matière de filtrage des flux de messagerie.

A.2. Coordonnées

Si vous avez des questions, vous pouvez vous adresser à nos distributeurs ou directement à Kaspersky Lab (en anglais). Nous vous garantissons un traitement détaillé de votre demande par téléphone ou par courrier électronique. Nous nous efforçons d'apporter des réponses complètes à vos questions.

Support technique	Pour une assistance technique, adressez-vous à : http://www.kaspersky.com/supportinter.html E-mail : france@support.kaspersky.com

Informations générales	WWW : http://www.kaspersky.com/fr/ Virus : http://www.viruslist.com/fr/ Support : http://support.kaspersky.fr E-mail : sales@kaspersky.fr

ANNEXE B. CONTRAT DE LICENCE

NOTE A TOUS LES UTILISATEURS : VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT DE LICENCE (« LICENCE ») SUIVANT, À PROPOS DE CE LOGICIEL (« LOGICIEL ») FABRIQUÉ PAR KASPERSKY LAB. (« KASPERSKY LAB »).

L'ACQUISITION DE CE LOGICIEL VIA INTERNET A LA SUITE D'UN CLIC SUR LE BOUTON ACCEPTER SIGNIFIE QUE VOUS (PARTICULIER OU ENTITÉ INDIVIDUELLE) ACCEPTEZ DE RESPECTER ET DE DEVENIR PARTIE DE CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, CLIQUEZ SUR LE BOUTON INDIQUANT QUE VOUS N'ACCEPTEZ PAS LES TERMES DE CE CONTRAT ET QUE VOUS N'INSTALLEZ PAS LE LOGICIEL.

SI VOUS AVEZ ACHETE CE LOGICIEL SOUS FORME PHYSIQUE, EN OUVRANT LE SCELLÉ DU BOÎTIER, VOUS (PARTICULIER OU ENTITÉ INDIVIDUELLE) ACCEPTEZ DE RESPECTER CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, N'OUVREZ PAS LE BOÎTIER DU CD, NE TELECHARGEZ, N'INSTALLEZ OU N'UTILISEZ PAS CE LOGICIEL. SI LE SCELLÉ EST DÉCHIRÉ OU LE BOÎTIER A ÉTÉ OUVERT, VOUS N'AUREZ PAS DROIT AU REMBOURSEMENT DU LOGICIEL. LES LOGICIELS POUR USAGE DOMESTIQUE (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY SECURITY FOR PDA) ACHETÉS SOUS FORME DE TÉLÉCHARGEMENT PAR INTERNET PEUT ETRE RETOURNE, ET REMBOURSÉ INTEGRALEMENT DANS LES 14 JOURS APRÈS SON ACHAT, À KASPERSKY LAB, SES REVENDEURS ET DISTRIBUTEURS AGREES. AUTRES PRODUITS NON REMBOURSABLES. LE DROIT AU RETOUR ET AU REMBOURSEMENT NE S'APPLIQUE QU'A L'ACHETEUR INITIAL.

Toutes les références au "Logiciel" apparaissant dans le présent contrat de licence incluent la clé d'activation (Fichier Clé d'Identification) qui sera fournie par Kaspersky Lab comme faisant partie du logiciel.

1. Licence de droits. Sous réserve d'acceptation des termes de la présente Licence d'utilisation et du paiement du prix d'achat du logiciel, Kaspersky Lab vous autorise à utiliser une copie unique et non transférable de la version spécifiée de ce logiciel et de la documentation (la « Documentation ») selon les termes de ce Contrat uniquement pour un usage interne à l'entreprise. Vous pouvez installer une copie du logiciel sur votre système. Si la licence concerne une suite d'applications (plus d'un seul logiciel), cette licence

s'applique à tous les logiciels de la suite, en respectant toute restriction ou limite d'utilisation spécifiée dans la liste de prix ou pour chaque paquet d'applications.

1.1 Utilisation. Ce logiciel ne peut être installé que sur un seul système (un seul ordinateur) par le client, et la licence d'utilisation n'est octroyée qu'à un utilisateur unique, sauf stipulation contraire dans cette Section.

1.1.1 Le Logiciel est dit « utilisé » sur un système client lorsqu'il est chargé dans la mémoire tampon (mémoire vive ou RAM) ou installé dans une mémoire permanente (par ex. disque dur, CD-ROM ou autre périphérique de stockage) de ce système client. La présente licence vous autorise à réaliser une copie unique du logiciel dans son intégralité à des fins de sauvegarde, à condition que les copies contiennent toutes les notices de propriété du Logiciel. Il vous incombe en outre de garder une trace de toute copie du logiciel et de sa documentation réalisée à des fins de sauvegarde et de prendre les précautions nécessaires pour qu'aucune autre copie et qu'aucune utilisation illégale ne soit effectuée.

1.1.2 Si vous cédez le Système Client sur lequel le Logiciel est installé, vous devrez au préalable vous assurer que toutes les copies du Logiciel ont été désinstallées.

1.1.3 Il est interdit de décompiler, faire de l'ingénierie inverse, désassembler ou altérer autrement toute partie de ce Logiciel sous forme lisible par l'homme, ni de permettre à un tiers de le faire. Les informations d'interface nécessaires pour réaliser l'interopérabilité du Logiciel avec des programmes informatiques indépendants seront fournies par Kaspersky Lab contre une rémunération en rapport avec le coût et les dépenses qu'impliquent de telles informations. Au cas où Kaspersky Lab vous informerait qu'il ne souhaite pas vous fournir de telles informations pour n'importe quelle raison, incluant les coûts (sans limitation), vous serez autorisé à réaliser l'interopérabilité à condition que vous ne fassiez pas d'ingénierie amont ou de décompilation hors les limites autorisées par la loi.

1.1.4 Il vous est interdit ainsi qu'à vos tiers de copier (au-delà de ce qui est permis expressément ici), d'apporter des corrections ou de modifier, adapter ou traduire le Logiciel, de produire des applications dérivées.

1.1.5 Il est interdit de louer ou de prêter le Logiciel à un tiers ou de transférer la licence et votre droit d'utilisation à un tiers.

1.1.6 Vous ne pourrez pas utiliser ce Logiciel avec des outils automatiques, semi-automatiques ou manuels conçus pour créer des signatures de virus, des routines de détection de virus ou tout autre code de détection de code ou de données dangereuses.

1.2 Utilisation en Mode Serveur. Vous devez utiliser le Logiciel sur un Système Client ou sur un serveur (« Serveur ») dans un environnement multi-utilisateurs ou en réseau (« Mode-Serveur ») uniquement si une telle utilisation est autorisée dans le tarif en vigueur ou sur l'emballage du Logiciel. Une licence spécifique est nécessaire pour chaque Système Client ou « poste », sans tenir compte du fait que ces systèmes autorisés ou ces postes sont connectés simultanément ou réellement en train d'utiliser le logiciel. L'utilisation de logiciels ou de matériels permettant de réduire le nombre de dispositifs client ou de postes utilisant le Logiciel (par exemple, par "multiplexage" ou "sondage" du logiciel ou du matériel) ne réduit pas le nombre de licences nécessaires : le nombre de licences requises égale le nombre d'entrées séparées gérées en interface par le programme ou matériel multiplexeur ou de sondage. Si le nombre de Systèmes Clients ou postes pouvant se connecter au Logiciel peut dépasser le nombre de licences dont vous disposez, il vous incombe de prendre des mesures raisonnables pour vous assurer que l'utilisation du Logiciel ne dépasse pas les limites d'utilisation spécifiées dans la licence obtenue. La présente licence vous autorise à télécharger ou à effectuer autant de copies de la documentation que le réseau compte de Clients possédant une licence d'utilisation du logiciel, à condition que la documentation contienne toutes les mentions de propriété légale.

1.3 Licences par volume. Si le Logiciel est inscrit avec des termes de Licences de volume spécifiés sur la facture en vigueur ou l'emballage du Logiciel, vous devez effectuer, utiliser ou installer autant de copies additionnelles du Logiciel sur le nombre de Systèmes Clients que les termes de la licence de volume le spécifient. Vous devez tout mettre en œuvre pour vous assurer que le nombre de Systèmes Clients sur lesquels le Logiciel a été installé ne dépasse pas le nombre de licences obtenues. Ce permis vous autorise à tirer ou télécharger une copie de la documentation pour chaque copie additionnelle autorisée par le permis de volume, à condition que chaque copie contienne toutes les notices de propriété industrielle du document.

2. Durée. Ce Contrat de Licence est valable pour la durée prévue par le fichier de clé (le fichier unique nécessaire pour activer complètement le Logiciel : reportez-vous au menu Aide/ À propos du logiciel ; pour la version Unix/Linux, consultez la note sur la date d'expiration du fichier de clé) à moins qu'il n'arrive à terme avant ce délai pour l'une des raisons prévues ci-après. Ce Contrat se terminera automatiquement si vous n'en respectez pas les termes, les limites ou les conditions décrites. Dans ce cas, il vous incombe de détruire toute copie du logiciel et de sa documentation que vous auriez réalisée. Vous pouvez mettre un terme à ce contrat à tout moment en détruisant les copies du logiciel et de sa documentation.

3. Support technique.

(i) Kaspersky Lab fournira une assistance technique (« Support ») comme décrit ci-dessous pour une période d'un an :

(a) le paiement des frais de l'assistance technique en cours ait été fait, et ;

(b) à la condition qu'ait été rempli le Formulaire d'inscription au Support Technique (Bon d'enregistrement) fourni avec le produit ou disponible sur le site Web de Kaspersky Lab, et qui nécessitera que vous communiquiez le Fichier Clé d'Identification fourni par Kaspersky Lab avec le présent Contrat de Licence. Il restera à l'entière discrétion de Kaspersky Lab de juger si vous remplissez les conditions d'accès prévues aux services de support technique.

(ii) Le support technique se termine sauf si renouvelée annuellement par le paiement des droits requis et par l'envoi d'un nouveau Formulaire d'Inscription.

(iii) En remplissant le Formulaire d'Inscription de l'Assistance Technique, vous acceptez les termes de la Stratégie de Confidentialité de Kaspersky Lab jointe à ce Contrat, et vous consentez explicitement au transfert de données vers d'autres pays que le vôtre, en accord avec les termes de la Stratégie de Confidentialité.

(iv) Le « service de support technique » comprend :

(a) Mises à jour quotidienne de la base antivirus ;

(b) Mises à jour logicielles gratuites, y compris les mises à niveau de la version ;

© Support technique avancé par courrier électronique et par téléphone, assuré par le revendeur ou le distributeur.

(d) Mises à jour de détection et d'éradication de virus par intervalles de 24 heures.

4. Droits de propriété. Le logiciel est protégé par les lois sur le copyright. Kaspersky Lab et ses fournisseurs conservent tous les droits de propriété applicables au logiciel. Le fait que vous en possédiez une copie et que vous l'ayez installée ne vous donne aucun droit de propriété intellectuelle sur le logiciel.

5. Confidentialité. Vous acceptez que le logiciel, toutes ses applications et le Fichier Clé d'Identification constituent des informations confidentielles dont Kaspersky Lab reste propriétaire. Vous ne dévoilerez pas et ne fournirez en

aucun cas ces informations confidentielles sous quelque forme que ce soit à un tiers sans l'autorisation expresse et écrite de Kaspersky Lab. Vous mettrez en œuvre des mesures de sécurité minimale visant à assurer que la confidentialité du Fichier Clé d'Identification est respectée, sans pour autant compromettre les conditions précédentes.

6. Limite de garantie

(i) Kaspersky Lab garantit que pour une durée de [90] jours suivant le téléchargement ou l'installation du logiciel, ce dernier fonctionnera correctement comme décrit dans la documentation fournie, et ce, lors d'une utilisation conforme et selon la manière spécifiée dans la Documentation.

(ii) Vous assumez l'entière responsabilité du choix du logiciel comme répondant à vos besoins. Kaspersky Lab ne garantit pas que le logiciel et sa documentation répondront à ces besoins et que leur utilisation sera exempte d'interruptions ou d'erreurs.

(iii) Kaspersky Lab ne garantit pas que ce Logiciel reconnaîtra tous les virus connus ou n'affichera pas de message de détection erroné ;

(iv) La responsabilité de Kaspersky Lab ne sera engagée qu'en cas de manquement au paragraphe (i), et il restera à la discrétion de Kaspersky Lab de réparer, remplacer ou rembourser le logiciel si le problème est signalé directement à Kaspersky Lab ou à un représentant au cours de la période de garantie. Vous devrez fournir toutes les informations nécessaires au fournisseur pour remédier à tout problème éventuel.

(v) La garantie comme décrite au paragraphe (i) ne s'appliquera pas si (a) vous modifiez ou faites modifier le logiciel sans le consentement de Kaspersky Lab, (b) vous utilisez le Logiciel d'une façon différente de son but initial ou (c) vous utilisez le Logiciel d'une façon non prévue par ce Contrat ;

(vi) Les garanties et conditions fixées dans ce Contrat prévalent sur toutes autres conditions et garanties légales ou termes qui concernent la fourniture ou la prétendue fourniture, le manquement ou délai à fournir le Logiciel ou la Documentation, mais qui pour ce paragraphe (v) ont effet entre Kaspersky Lab et vous ou sont implicites ou intégrés dans ce Contrat ou autre contrat collatéral, soit par statut, loi commune ou tout ce qui est exclu ici (incluant sans limitation les conditions, garanties ou autres termes relatifs à la qualité de satisfaction, justesse d'utilisation ou pour le respect de compétences et du bon sens).

7. Décharge de responsabilité

(i) Rien dans ce Contrat ne saurait engager la responsabilité de Kaspersky Lab en cas (i) de non-satisfaction de l'utilisateur, (ii) de décès ou dommages physiques résultant d'infractions aux lois en vigueur et du non-respect des termes de ce Contrat, (iii) de toute infraction aux obligations impliquées par la loi « s.12 Sale of Goods Act 1979 or s.2 Supply of Goods and Services Act 1982 » ou (iv) de responsabilité qui ne peut être exclue par la loi.

(ii) Selon les termes du paragraphe (i), le Fournisseur ne pourra être tenu pour responsable (si dans le contrat, acte dommageable, compensation ou autres) pour les dommages et pertes suivants (si de tels dommages ou pertes étaient prévus, prévisibles, connus ou autres) :

(a) Perte de revenus ;

(b) Perte de revenus réels ou potentiels (incluant les pertes de revenus sur contrats) ;

© Perte de moyens de paiement ;

(d) Perte d'économies prévues ;

(e) Perte de marché ;

(f) Perte d'occasions commerciales ;

(g) Perte d'image ;

(h) Perte de réputation ;

(i) Perte, endommagement ou corruption des données ; ou

(j) Tout dommage ou toute perte qu'ils soient directs ou indirects, ou causés de quelque façon que ce soit (incluant, pour éviter le doute, ces dommages ou pertes spécifiés dans les paragraphes (ii), (a) jusque (ii), (i).

(iii) Selon les termes du paragraphe (i), la responsabilité de Kaspersky Lab (suite au contrat, acte dommageable, compensation ou autres) survenant lors de la fourniture du Logiciel n'excèdera en aucun cas un montant égal au prix d'achat du Logiciel.

8. L'interprétation du présent Contrat de Licence sera effectuée en accord avec la législation locale. Les parties se soumettent ici à la juridiction des cours d'Angleterre et du Pays de Galles, sauf si Kaspersky Lab était autorisé en tant que requérant à entamer des poursuites auprès de n'importe quelle juridiction compétente.

9. (i) Le présent Contrat de Licence constitue l'accord unique liant les parties et prévaut sur tout autre arrangement, promesse ou accord verbal ou écrit passé au préalable entre vous et Kaspersky Lab ou l'un de ses

représentants. En dehors des situations prévues dans les paragraphes (ii) - (iii), vous n'aurez aucune possibilité de recours contre Kaspersky Lab au cas où vous auriez fourni des informations erronées dans le cadre du présent Contrat de Licence. En dehors des situations prévues par les paragraphes (ii) – (iii), vous n'aurez aucun recours au cas où vous auriez fourni des informations erronées et sur lesquelles vous vous basiez en acceptant ce Contrat (« Fausse Représentation ») et Kaspersky Lab ne sera pas tenu pour responsable envers tout autre poursuivant que celui déterminé.

(ii) Rien dans ce Contrat ne pourra limiter ou exclure la responsabilité de Kaspersky Lab pour toute Fausse Représentation faite en connaissance de cause.

(iii) La responsabilité de Kaspersky Lab pour Fausse Déclaration portant sur une question fondamentale, y compris pour l'obligation du fabricant de respecter ses engagements au titre de ce Contrat, sera sujette à la décharge de responsabilité du paragraphe 7 (iii).