

KASPERSKY LAB

---

Kaspersky Anti-Virus 5.0 for  
MIMESweeper

ADMINISTRATOR'S  
GUIDE

KASPERSKY ANTI-VIRUS 5.0 FOR MIMESWEEPER 5.X

---

# Administrator's Guide

© Kaspersky Lab

<http://www.kaspersky.com>

Revision date: August 2006

# Table of contents

CHAPTER 1. INTRODUCTION .....	4
CHAPTER 2. HARDWARE AND SOFTWARE SYSTEM REQUIREMENTS.....	5
CHAPTER 3. INSTALLING KASPERSKY ANTI-VIRUS FOR MIMESWEEPER .....	6
CHAPTER 4. USING KASPERSKY ANTI-VIRUS .....	7
4.1. Configuring updates to the anti-virus database.....	7
4.2. Update servers of Kaspersky Lab.....	8
4.3. Using GUI to configure updates.....	9
4.3.1. Configuring the connection parameters.....	9
4.3.2. Scheduling updates .....	10
4.3.3. Selecting the source of updates.....	11
4.3.4. Selecting the update folders.....	12
4.4. Interaction between MIMESweeper and Kaspersky Anti-Virus .....	14
4.4.1. MIMESweeper policy editor .....	14
4.4.2. MIMESweeper scenarios.....	14
4.4.3. Configuring the content scanning scenario .....	15
CHAPTER 5. TESTING THE KASPERSKY ANTI-VIRUS OPERATION.....	16
CHAPTER 6. LICENSING .....	18
6.1. Overview .....	18
6.2. Validity period of commercial keys.....	18
APPENDIX A. GLOSSARY .....	19
APPENDIX B. KASPERSKY LAB.....	20
B.1. Other Kaspersky Lab Products .....	21
Contact Us .....	28
APPENDIX C. LICENSE AGREEMENT .....	30

---

# CHAPTER 1. INTRODUCTION

Kaspersky Anti-Virus for MIMESweeper is intended for real-time anti-virus protection of incoming and outgoing e-mail transferred through Clearswift MIMESweeper for SMTP.

Kaspersky Anti-Virus for MIMESweeper offers the following features:

- Interception of incoming and outgoing mail messages.
- Scanning of message stream for virus presence.
- Anti-virus processing of infected parts in mail messages revealed during scanning.
- Generation of statistics and reports on application activity.
- Automatic updates to the anti-virus database and program modules.

---

# CHAPTER 2. HARDWARE AND SOFTWARE SYSTEM REQUIREMENTS

Kaspersky Anti-Virus for MIMESweeper supports Clearswift MIMESweeper for SMTP.

Clearswift developers have designed the software interfaces that provide for compatibility between their products and Kaspersky Anti-Virus for MIMESweeper.

These system requirements apply to Kaspersky Anti-Virus only. Requirements for Clearswift products and interfaces can be found in the documentation for CS MIMESweeper for SMTP. Kaspersky Anti-Virus can function on the server running Clearswift product (if the system requirements of that Clearswift product are identical to the requirements for Kaspersky Anti-Virus).

Hardware and software requirements:

- Microsoft Windows Server 2003 or Microsoft Windows 2000 Server or Advanced Server with Service Pack 2 or later.
- Intel Pentium III CPU.
- 256 Mb RAM.
- 25 Mb of available hard disk space.
- Internet connection necessary to download updates.

---

# CHAPTER 3. INSTALLING KASPERSKY ANTI-VIRUS FOR MIMESWEEPER

Kaspersky Anti-Virus MIMESweeper must always be installed to the computer running MIMESweeper for SMTP.

In order to install Kaspersky Anti-Virus for MIMESweeper perform the following steps:

1. Save the installation package to a temporary folder before setup start.
2. Read the information displayed on the welcome screen and click the **Next** button to continue.
3. Select the destination folder for product installation. Click the **Next** button to continue.
4. Click the **Close** button to finalize installation.

---

# CHAPTER 4. USING KASPERSKY ANTI-VIRUS

## 4.1. Configuring updates to the anti-virus database

Kaspersky Anti-Virus for MIMESweeper downloads updates to the anti-virus database automatically. Kaspersky Lab provides new updates every hour.

To ensure stable non-stop functioning of the anti-virus system, Kaspersky Anti-Virus for MIMESweeper arranges work of the components so as to prevent blocking the files of the anti-virus database by the processes of Kaspersky Anti-Virus engine as that could interfere with correct updating of these files.

Reliable protection of your computer depends on timely updates to anti-virus software. Since new viruses, trojans and other malicious applications appear every day, adequate security of your data requires regular updating of your anti-virus solution.

In order to download updates from the servers of Kaspersky Lab or other FTP or HTTP servers you are advised to check first your Internet connection settings. By default, the application establishes connection using the settings of your web browser (e.g., Microsoft Internet Explorer). To modify these settings, you will need technical information about an existing proxy server or installed firewall, if any. If you have no such information, please contact your system administrator or Internet service provider.

Updates can be downloaded from servers specified as the values for the **<update\_srv\_url>** parameter in the **<source>** section of the XML configuration file or the *updatersdk.xml* file.

The **<source>** section may contain one or several values for the **<update\_srv\_url>** parameter. Possible options:

1. The **<source>** section contains more than one value for the **<update\_srv\_url>** parameter. The updating routine will use the addresses specified in this section only.
2. The **<source>** section contains just one value for the **<update\_srv\_url>** parameter.
  - If **<inet\_update>=0** and **<try\_inet>=0**, then the updater module will use the address specified for **<update\_srv\_url>**.

- If **<inet\_update>=0** and **<try\_inet>=1**, then the updater module will use the address specified for **<update\_srv\_url>**. If an update attempt fails, the updater will try to access the addresses listed in *updcfg.xml*.
- If **<inet\_update>=1**, the updater will use the addresses from *updcfg.xml*.

The **<proxy>** section:

**proxy** – instruction to use a proxy server for Internet connection. If this option is set to **1**, a proxy is used.

**use\_ie\_proxy** – instruction to use the proxy settings from Microsoft Internet Explorer. If the option is set to **1**, the updater will use the settings of Microsoft Internet Explorer.

**proxy\_url** – proxy server address (as a character or numeric string).

**proxy\_port** – proxy server port.

**proxy\_authorization** – instruction to use proxy server authentication. Authentication is used if the option is set to **1**.

**proxy\_ntlm\_access\_token** – instruction to use NTLM authentication. NTLM authentication will be used with the specified proxy if the option is set to **1**. If it is set to **0**, basic authentication is used.

**proxy\_login** – proxy user name.

**proxy\_pwd** – proxy server password.

## 4.2. Update servers of Kaspersky Lab

HTTP and FTP servers, local and network folders can act as sources of updates. Updates can be downloaded from the following servers of Kaspersky Lab using HTTP/FTP:

- <http://downloads1.kaspersky-labs.com/>
- <http://downloads2.kaspersky-labs.com/>
- <http://downloads3.kaspersky-labs.com/>
- <http://downloads4.kaspersky-labs.com/>
- <http://downloads5.kaspersky-labs.com/>
- <ftp://downloads1.kaspersky-labs.com/>
- <ftp://downloads2.kaspersky-labs.com/>
- <ftp://downloads3.kaspersky-labs.com/>

- ftp://downloads4.kaspersky-labs.com/
- ftp://downloads5.kaspersky-labs.com/

## 4.3. Using GUI to configure updates

*Updconfg.exe* is a utility that can be used to modify the parameters used for updating of the anti-virus database. All settings of the updater module can be accessed from Microsoft Windows interface.

### 4.3.1. Configuring the connection parameters

You can use the **LAN Settings** tab (see Fig. 1) to modify the parameters used for network connection in order to download updates.

Enable the **Use passive FTP mode if possible** checkbox to download updates from an FTP server in passive mode (e.g., via a firewall). Uncheck the box if you are using active mode.

Enable the **Use proxy server** checkbox if the Internet connection must be established via a proxy server. Specify the proxy settings that will be used during updating:

- **Use IE proxy settings** – Microsoft Internet Explorer settings will be used during connection through the proxy.
- **Use custom proxy settings** – instruction to use proxy settings that differ from browser configuration. In the **Address** field enter the **IP** address or the name of the proxy server and use the **Port** field to specify the number of the port to be used for application updates.

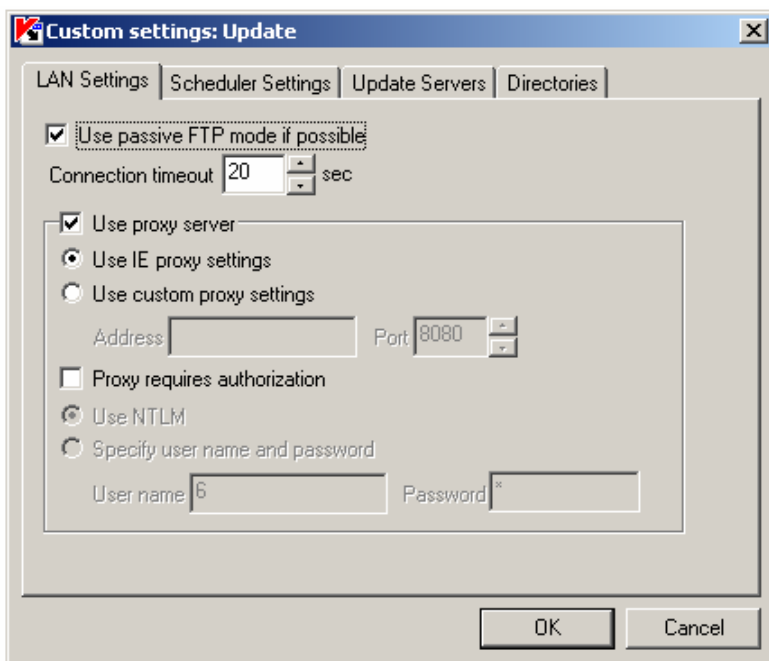


Figure 1. The **LAN Settings** tab

Enable the **Proxy requires authorization** checkbox if authorization is required to establish connection. Select the mode of authorization for the proxy server during establishment of an Internet connection:

- **Use NTLM** – instruction to use the information of the current user profile for connection to the Internet.
- **Specify user name and password** – instruction to substitute the user name and password entered in the corresponding fields.

### 4.3.2. Scheduling updates

Use the **Scheduler Settings** tab (see Fig. 2) to schedule the start of the updating task.

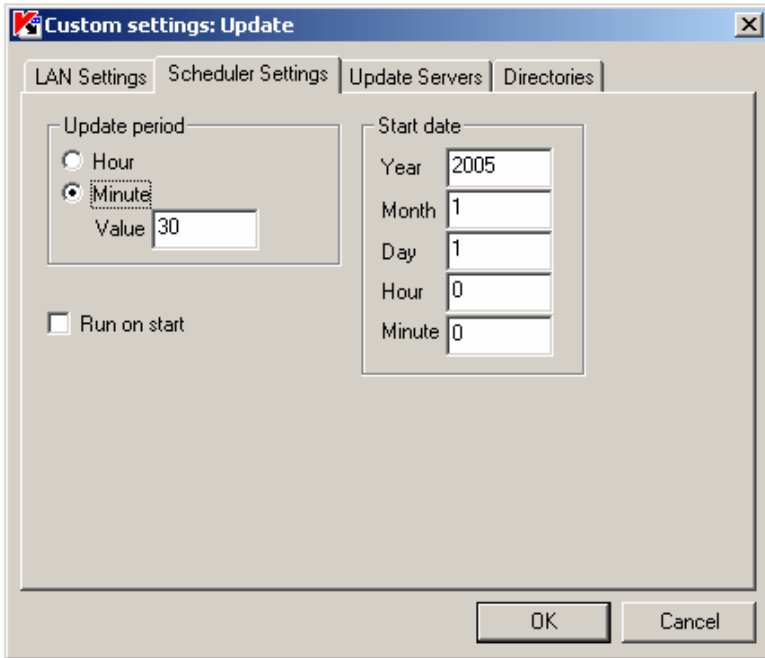


Figure 2. The **Scheduler Settings** tab

Specify the frequency that will be used to check for availability of updates:

- If **Hour** is selected, then availability of updates will be checked every n-th hour, where n stands for the number in the **Value** field.
- If **Minute** is selected, then availability of updates will be checked every n-th minute, where n stands for the number in the **Value** field.

If the **Run on start** checkbox is enabled, the updater will run automatically at each system start.

### 4.3.3. Selecting the source of updates

Server settings can be found in the **Update Servers** tab (see Fig. 3).

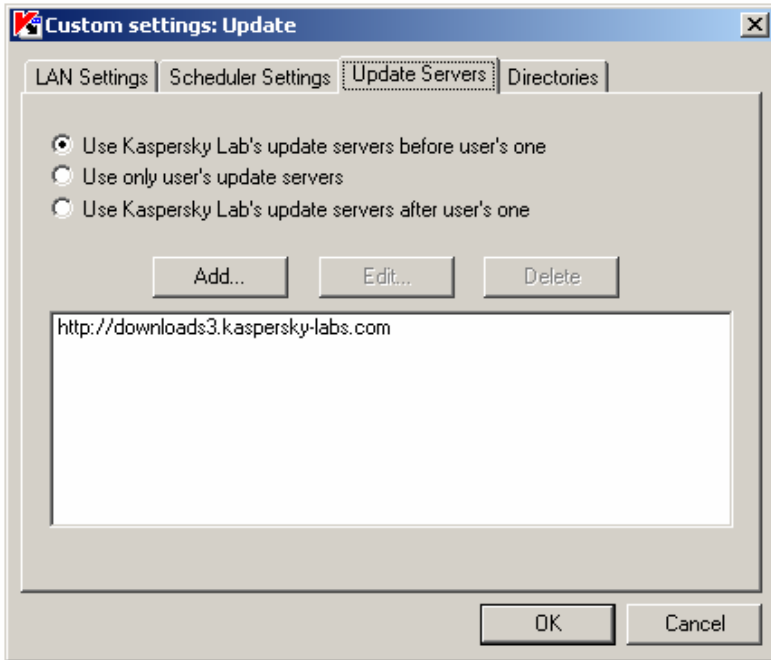


Figure 3. The **Update Servers** tab

Update servers of Kaspersky Lab act as the main source of updates (see section 4.2 on page 8).

In order to download available updates from the servers, your computer needs a properly configured Internet connection.

You can also select other servers for downloading of updates. In order to configure updating from other FTP or HTTP servers, perform the following steps:

- Click the **Add** button.
- Use the **Select an update source** window that open next to select an FTP or HTTP server or specify its IP address or URL in the **Source** field.
- Click the **OK** button.

#### 4.3.4. Selecting the update folders

All folders used by the updater module are listed in the **Directories** tab (see Figure 4).

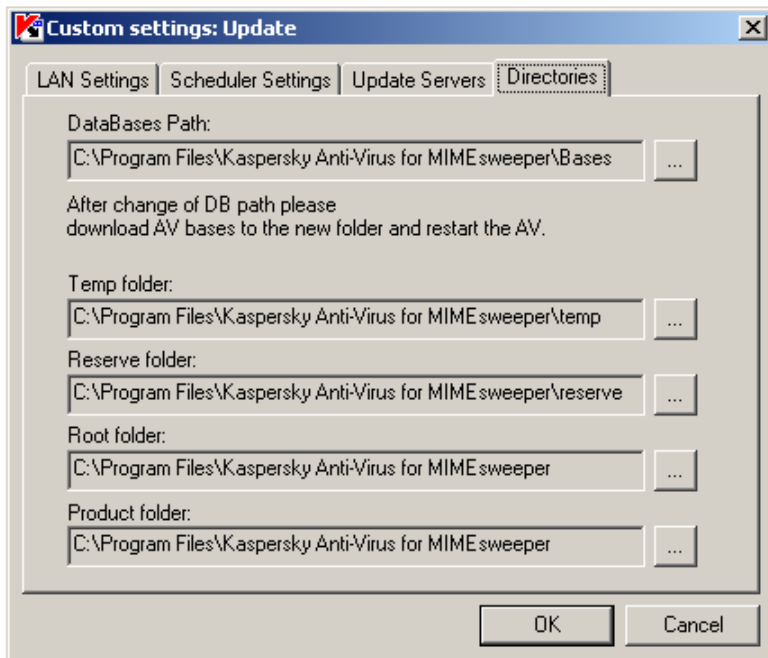


Figure 4. The **Directories** tab

You can modify the path for the following files and folders:

- Anti-virus database (DataBases Path).
- Folders for temporary files (Temp folder).
- Folders for backup storage (Reserve folder).
- Main program folder (Root folder).
- Folder containing the plug-in for the product (Product folder).

## 4.4. Interaction between MIMESweeper and Kaspersky Anti-Virus

MIMESweeper can be configured to scan just incoming/outgoing messages or all messages. Kaspersky Anti-Virus for MIMESweeper scans e-mail in real time. Therefore messages sent to several recipients will only be checked once.

While configuring Kaspersky Anti-Virus for MIMESweeper, you create scenarios used to check incoming and outgoing e-mail. These scenarios define the data formats that will be scanned. You can also configure the scanning of archives, such as ZIP and ARJ. Please refer to the documentation for MIMESweeper for detailed information.

### 4.4.1. MIMESweeper policy editor

Kaspersky Anti-Virus for MIMESweeper is configured using the MIMESweeper policy editor integrated into MMC (Microsoft Management Console). System administrators can use MMC to create a collection of integrated tools for performance of individual tasks, for example, anti-virus scanning.

### 4.4.2. MIMESweeper scenarios

In order to configure MIMESweeper for work with Kaspersky Anti-Virus, you have to create a scenario in MIMESweeper console. The scenario describes how MIMESweeper should scan data checking it for potential threats.

As soon as a MIMESweeper scenario involving Kaspersky Anti-Virus is created, a link between MIMESweeper and on-demand scanning module of Kaspersky Anti-Virus will be established. All messages processed in accordance with that scenario will also be checked by Kaspersky Anti-Virus.

Scenarios are stored as folders arranged in hierarchic order. A scenario in the upper level folder is referred to as global; it applies to all received or sent messages. You can create scenarios in child folders for more detailed message scanning. Further we shall describe the procedure for creation of a global MIMESweeper scenario that involves Kaspersky Anti-Virus. Detailed information about the procedure of scenario creation can be found in the Administrator's guide for MIMESweeper.

### 4.4.3. Configuring the content scanning scenario


*In order to configure a scenario for content scanning:*

1. Open the MIMESweeper console for SMTP.
2. Select **Incoming Scenario**, then select new **Content Scanner**.
3. Open the new **Content Scanner Wizard** and click **Next**.
4. Check the **Enabled** box in the **Content Scanner Wizard**. Click the **Next** button.
5. Select Kaspersky Anti-Virus for MIMESweeper and click the **Next** button.
6. Click the **Finish** button.

---

# CHAPTER 5. TESTING THE KASPERSKY ANTI-VIRUS OPERATION

After installing and configuring Kaspersky Anti-Virus, we recommend that you test the correctness of its settings and operation of the application using a test "virus" or its modifications.

The test virus was specially designed by the European Institute for Computer Antivirus Research organization , for testing anti-virus products.

The test "virus" IS NOT ACTUALLY A VIRUS because it does not contain code that can really harm your computer. However, most anti-virus products identify this file as a virus.



Never use real viruses for testing the operation of an anti-virus product!

You can download the test "virus" from the official website of the **EICAR** organization at [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).

The file downloaded from the **EICAR** website or created as described above contains the body of a standard test "virus". The anti-virus application will detect it, recognize it as **Infected** and incurable and apply the action defined by the administrator for handling objects belonging to that type.

To test the response of your anti-virus application to other types of objects, modify the body of this standard test "virus" by adding one of the prefixes listed in Table 1).



You can test the correctness of Kaspersky Anti-Virus operation using the modified EICAR "virus" only if your anti-virus database was last updated on or after October 24, 2003, or has the cumulative updates for October, 2003.

**Table 1. Test "virus" modifications**

Prefix	Object type
No prefix, standard test "virus"	Infected. The object cannot be cured.

Prefix	Object type
CORR–	Corrupted.
SUSP–	Suspicious (unknown viral code).
WARN–	Warning (modified code of a known virus).
ERRO–	Error when scanning the object.
CURE–	Infected. The object can be disinfected; the text in the "virus" body is replaced then with CURE.
DELE–	Infected. The object will be deleted automatically.

After adding a prefix to the test "virus" save it, for example, to a file under the name *eicar\_dele.com*; assign names to all the modified "viruses" in the same manner.

The second column of this table contains the types of objects identified by an anti-virus application after you have added a prefix. The actions for each type of objects are defined by anti-virus application settings customized by the administrator.



You are advised to check the Anti-Virus operation both with incoming and outgoing e-mail, with message bodies and attachments. To check virus detection in message body, add the text of a standard or modified test "virus" to message body.

---

# CHAPTER 6. LICENSING

## 6.1. Overview

Kaspersky Anti-Virus for MIMESweeper requires a valid license key. License key of Kaspersky Lab is a file containing information about the user, product, date of license expiry and other essential data. License keys of Kaspersky Lab are provided for each individual product.

Requests for scanning will not be served without a valid license key installed on a local drive or stored in the folder containing the files of Kaspersky Anti-Virus for MIMESweeper.

## 6.2. Validity period of commercial keys

Important aspects that affect the validity period of commercial license keys are as follows:

- **Key creation date** – date when a key has been generated.
- **Validity period** – the period during which the corresponding product of Kaspersky Lab can be used lawfully. The validity period is also referred to as the key validity period. Typically, the period lasts one or two years.
- **Installation period** – time period beginning with the date of key creation. If a key is used for product activation within the installation period, the license will be available throughout the whole validity period. Otherwise the duration of full product functionality will become shorter.
- **Expiry** – time when your license expires. Its duration cannot exceed **[validity period] + [installation period]**.

---

## APPENDIX A. GLOSSARY

**KAV (Kaspersky AV) Engine** – the core of Kaspersky Anti-Virus. It is the basic technology used in all products of Kaspersky Anti-Virus.

**Anti-Virus Database (AV DB)** – a collection of files containing signatures of known viruses and algorithms of their detection.

**Anti-Virus Database Update (process)** – the process used to deliver new anti-virus database files from a remote server to a local computer, for example to end user system or to a partner mirror server. During an update the anti-virus may transfer a complete set of anti-virus databases or just their new parts in order to minimize network traffic.

**AV functionality** – main features of the applications are scanning of files for virus presence and removal of viruses, updating of the anti-virus databases, support, etc.

---

## APPENDIX B. KASPERSKY LAB

Founded in 1997, Kaspersky Lab has become a recognized leader in information security technologies. It produces a wide range of data security software and delivers high-performance, comprehensive solutions to protect computers and networks against all types of malicious programs, unsolicited and unwanted e-mail messages, and hacker attacks.

Kaspersky Lab is an international company. Headquartered in the Russian Federation, the company has representative offices in the United Kingdom, France, Germany, Japan, USA (CA), the Benelux countries, China, Poland, and Romania. A new company department, the European Anti-Virus Research Centre, has recently been established in France. Kaspersky Lab's partner network incorporates more than 500 companies worldwide.

Today, Kaspersky Lab employs more than 450 specialists, each of whom is proficient in anti-virus technologies, with 10 of them holding M.B.A. degrees, 16 holding Ph.Ds, and senior experts holding membership in the Computer Anti-Virus Researchers Organization (CARO).

Kaspersky Lab offers best-of-breed security solutions, based on its unique experience and knowledge, gained in over 14 years of fighting computer viruses. A thorough analysis of computer virus activities enables the company to deliver comprehensive protection from current and future threats. Resistance to future attacks is the basic policy implemented in all Kaspersky Lab's products. At all times, the company's products remain at least one step ahead of many other vendors in delivering extensive anti-virus coverage for home users and corporate customers alike.

Years of hard work have made the company one of the top security software manufacturers. Kaspersky Lab was one of the first businesses of its kind to develop the highest standards for anti-virus defense. The company's flagship product, Kaspersky Anti-Virus, provides full-scale protection for all tiers of a network, including workstations, file servers, mail systems, firewalls, Internet gateways, and hand-held computers. Its convenient and easy-to-use management tools ensure advanced automation for rapid virus protection across an enterprise. Many well-known manufacturers use the Kaspersky Anti-Virus kernel, including Nokia ICG (USA), F-Secure (Finland), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India) and BorderWare (Canada).

Kaspersky Lab's customers benefit from a wide range of additional services that ensure both stable operation of the company's products, and compliance with specific business requirements. Kaspersky Lab's anti-virus database is updated every hour. The company provides its customers with a 24-hour technical support service, which is available in several languages to accommodate its international clientele.

## B.1. Other Kaspersky Lab Products

### Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus® Personal has been designed to provide anti-virus protection to personal computers running Microsoft Windows 98/ME or Microsoft Windows 2000/NT/XP against all known viruses, including potentially dangerous software. Kaspersky Anti-Virus Personal provides real-time monitoring of all sources of virus intrusion - e-mail, Internet, floppy disks, CD, etc. The unique system of heuristic data analysis allows efficient neutralization of yet unknown viruses. This application can work in the following modes (that can be used separately or jointly):

- **Real-time computer protection** - anti-virus scanning of all objects run, opened on or saved to the user's computer.
- **On-demand computer scan** - scanning and disinfection of the entire user's computer or of individual disks, files or folders. You can start such scan manually or configure an automatic scheduled scan.

Kaspersky Anti-Virus® Personal does not re-scan objects that had already been scanned during a previous scan and have not changed since then not only when performing real-time protection, but also during an on-demand scan. This feature **considerably increases the speed of the program's operation.**

The application creates a reliable barrier against viruses when they attempt to intrude your computer via e-mail. Kaspersky Anti-Virus® Personal performs automatic scan and disinfection of all incoming and outgoing mail sent or received using POP3 and STMP protocols and provides highly efficient detection of viruses in mail databases.

The application supports over 700 formats of archived and compressed files and provides automatic scanning of their content as well as removal of malicious code from **ZIP, CAB, RAR, ARJ, LHA** and **ICE** archives.

Configuring the application is made simple and intuitive due to the possibility to select one of three preset protection levels: **Maximum Protection, Recommended** or **High Speed.**

The anti-virus database is updated every hour and its delivery to your computer is guaranteed even when your computer gets temporarily disconnected from the Internet or the connection has to be changed.

### Kaspersky Anti-Virus® Personal Pro

This package has been designed to deliver comprehensive anti-virus protection to home computers running Microsoft Windows 98/ME, Microsoft Windows 2000/NT, Microsoft Windows XP as well as MS Office applications. Kaspersky Anti-Virus Personal Pro includes an easy-to-use application for automatic retrieval of daily updates for the anti-virus database and the program modules. A

unique second-generation heuristic analyzer efficiently detects unknown viruses. A simple and convenient interface allows users to configure the program quickly making work with it easier than ever.

Kaspersky Anti-Virus® Personal Pro has the following features:

- **On-demand scan** of local disks.
- **Real-time automatic protection** of all accessed files from viruses.
- **Mail Filter** automatically scans and disinfects all incoming and outgoing mail for any mail client that uses POP3 and SMTP protocols and effectively detects viruses in mail databases.
- **Behavior blocker** that provides maximum protection of MS Office applications against viruses.
- **Archive scanning** – Kaspersky Anti-Virus recognizes over 900 formats of archived and compressed files and ensures automatic anti-virus scanning of their content and removal of malicious code from files within **ZIP, CAB, RAR, ARJ, LHA** and **ICE** archives.

### **Kaspersky® Anti-Hacker**

Kaspersky® Anti-Hacker is a personal firewall that is designed to safeguard a computer running any Microsoft Windows operating system. It protects your computer against unauthorized access and external hacker attacks from either the Internet or the local network.

Kaspersky® Anti-Hacker monitors the TCP/IP network activity of all applications running on your machine. When it detects a suspicious action, Kaspersky® Anti-Hacker blocks the suspicious application from accessing the network. This helps ensure enhanced privacy and 100% security of confidential data stored on your computer.

The product's SmartStealth™ technology prevents hackers from detecting your computer from the outside. In this stealthy mode, the application works seamlessly to keep your computer protected while you are on the Web. The application provides conventional transparency and accessibility of information.

Kaspersky® Anti-Hacker also blocks most common network hacker attacks and monitors attempts to scan computer ports.

Configuration of the application is simply a matter of choosing one of five security levels. By default, the application starts in self-learning mode, which will automatically configure your security system depending on your responses to various events. This makes your personal guard adjustable to your specific preferences and your particular needs.

### **Kaspersky® Personal Security Suite**

Kaspersky® Personal Security Suite is a software suite designed for organizing comprehensive protection of personal computers running Microsoft Windows.

The suite prevents malicious and potentially dangerous programs from penetrating through any possible data sources and protects you from unauthorized attempts to access your computer's data, as well as blocking spam.

Kaspersky Personal Security Suite has the following features:

- anti-virus protection of data saved on your computer
- protection against spam for users of Microsoft Office Outlook and Microsoft Outlook Express
- protection of your computer from unauthorized access, and also from network hacker attacks from your LAN or the Internet.

### **Kaspersky Lab News Agent**

The News Agent is intended for timely delivery of news published by Kaspersky Lab, for notifications about the current status of virus activity and fresh news. The program reads the list of available news channels and their content from news server of Kaspersky Lab with specified frequency.

The product performs the following functions:

- It visualizes in the system tray the current status of virus activity.
- The product allows the users to subscribe and unsubscribe from news channels.
- It retrieves news from each subscribed channel with the specified frequency and notifies about fresh news.
- It allows reviewing news on the subscribed channels.
- It allows reviewing the list of channels and their status.
- It allows opening pages with news details in your browser.

News Agent is a stand-alone Microsoft Windows application, which can be used independently or may be bundled with various integrated solutions offered by Kaspersky Lab Ltd.

### **Kaspersky® OnLine Scanner**

The program is a free service offered to the visitors of Kaspersky Lab's corporate website. The service allows an efficient online anti-virus scan of your computer. Kaspersky OnLine Scanner runs within your web browser using Microsoft ActiveX® technology. Thus, users can quickly test their computers in case of a slightest suspicion of malicious infection. Using the service, visitors can:

- Exclude archives and e-mail databases from scanning.
- Select standard/extended anti-virus databases for scanning.
- Save a report on the scanning results in txt or html formats.

## Kaspersky® OnLine Scanner Pro

The program is a subscription service offered to the visitors of Kaspersky Lab's corporate website. The service allows an efficient online anti-virus scan of your computer and disinfection of dangerous files. Kaspersky OnLine Scanner Pro runs within your web browser using Microsoft ActiveX® technology. Using the service, visitors can:

- Exclude archives and e-mail databases from scanning.
- Select standard/extended anti-virus databases for scanning.
- Save a report on the scanning results in txt or html formats.

## Kaspersky Anti-Virus® 6.0

Kaspersky Anti-Virus 6.0 is designed to safeguard personal computers against malicious software as an optimal combination of conventional methods of anti-virus protection and new proactive technologies.

The program provides for complex anti-virus checks including:

- Anti-virus scanning of e-mail traffic on the level of data transmission protocol (POP3, IMAP and NNTP for incoming mail and SMTP for outgoing messages) irrespectively of the mail client being used as well as disinfection of e-mail databases.
- Real-time anti-virus scanning of Internet traffic transferred via HTTP.
- Anti-virus scanning of individual files, directories or drives. In addition, a preset scan task can be used to initiate anti-virus analysis exclusively for critical areas of the operating system and start-up objects of Microsoft Windows.

Proactive protection offers the following features:

- **Control of changes within file system.** The program allows users to create a list of applications, which it will control on a per component basis. It helps protect application integrity against the influence of malicious software.
- **Monitoring of processes in random-access memory.** Kaspersky Anti-Virus 6.0 in a timely manner notifies users whenever it detects dangerous, suspicious or hidden processes or in case when unauthorized changes in standard processes occur.
- **Monitoring of changes in OS registry** due to internal system registry control.
- **Blocking of dangerous VBA macros** in Microsoft Office documents.
- **System restoration** after malicious spyware influence accomplished due to recording of all changes in the registry and computer file system and an opportunity to perform their roll-back at user's discretion.

## Kaspersky® Internet Security 6.0

Kaspersky® Internet Security 6.0 is an integrated solution for protection of personal computers against the main information-related threats, i.e. viruses, hackers, spam and spyware. A common user interface allows configuration and management of all solution components.

The anti-virus protection feature includes:

- **Anti-virus scanning of e-mail traffic** on the level of data transmission protocol (POP3, IMAP and NNTP for incoming mail and SMTP for outgoing messages) irrespectively of the mail client being used. The program includes plug-ins for popular e-mail clients (Microsoft Office Outlook, Microsoft Outlook Express and The Bat!) and supports disinfection of their e-mail databases.
- **Real-time anti-virus scanning of Internet traffic** transferred via HTTP.
- **File system protection:** anti-virus scanning of individual files, directories or drives. In addition, the application can perform anti-virus analysis exclusively for critical areas of the operating system and start-up objects of Microsoft Windows.
- **Proactive protection:** the program performs constant monitoring of application activity and processes running in random-access memory preventing dangerous changes to the file system and registry, and restores the system after malicious influence.

**Protection against Internet-fraud** is guaranteed owing to the ability to recognize phishing attacks, which helps prevent confidential data leaks (first of all, your passwords, bank account and credit card numbers), and block execution of dangerous scripts on web pages, pop-up windows and advertisement banners. The feature **blocking charged phone calls** helps identify software that attempts to use your modem for hidden unauthorized connection to paid phone services and prevents such activity.

Kaspersky® Internet Security 6.0 **registers attempts to scan the ports of your computer**, which frequently precede network attacks, and successfully defends against typical hacker attacks. The program uses **defined rules as a basis** for control over all network transactions tracking all **incoming and outgoing data packets**. **Stealth mode** (owing to the SmartStealth™ technology) **prevents computer detection from outside**. When you switch into that mode, the system will block all network activity except for a few transactions allowed in user-defined rules.

The program employs complex approach to anti-spam filtering of incoming e-mail messages:

- Verification against black and white lists of recipients (including addresses of phishing sites).
- Inspection of phrases in message body.

- Analysis of message text using a self-learning algorithm.
- Recognition of spam sent in image files.

### **Kaspersky® Security for PDA**

Kaspersky® Security for PDA provides reliable anti-virus protection for data saved on various types of hand-held computers and smartphones. The program includes an optimal set of anti-virus defense tools:

- **anti-virus scanner** that scans information (saved both in internal memory of PDA and smartphones or on memory cards of any type) on user demand;
- **anti-virus monitor** to intercept viruses in files that are either copied from other handhelds or are transferred using HotSync™ technology.

Kaspersky® Security for PDA protects your handheld (PDA) from unauthorized intrusion by encrypting both access to the device and data stored on memory cards.

### **Kaspersky Anti-Virus® Business Optimal**

This package provides a unique configurable security solution for small- and medium-sized corporate networks.

Kaspersky Anti-Virus® Business Optimal guarantees full-scale anti-virus protection<sup>1</sup> for:

- *Workstations* running Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation and Linux.
- *File servers* running Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Microsoft Windows 2003 Server, Novell Netware, FreeBSD and OpenBSD, Linux, Samba Servers.
- *E-mail systems* including Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail, and Qmail.
- *Internet gateways*: CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition.

The Kaspersky Anti-Virus® Business Optimal distribution kit includes Kaspersky® Administration Kit, a unique tool for automated deployment and administration.

You are free to choose from any of these anti-virus applications, according to the operating systems and applications you use.

---

<sup>1</sup> Depending on the type of distribution kit.

## Kaspersky® Corporate Suite

This package provides corporate networks of any size and complexity with comprehensive, scalable anti-virus protection. The package components have been developed to protect every tier of a corporate network, even in mixed computer environments. Kaspersky® Corporate Suite supports the majority of operating systems and applications installed across an enterprise. All package components are managed from one console and have a unified user interface. Kaspersky® Corporate Suite delivers a reliable, high-performance protection system that is fully compatible with the specific needs of your network configuration.

Kaspersky® Corporate Suite provides comprehensive anti-virus protection for:

- *Workstations* running Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation and Linux;
- *File servers* running Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD, Linux and Samba Servers;
- *E-mail systems*, including Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim and Qmail;
- *Internet gateways*: CheckPoint Firewall –1; Microsoft ISA Server 2004 Enterprise Edition;
- *Hand-held computers* (PDAs), running Microsoft Windows CE and Palm OS, and also smartphones running Microsoft Windows Mobile 2003 for Smartphone and Microsoft Smartphone 2002.

The Kaspersky® Corporate Suite distribution kit includes Kaspersky® Administration Kit, a *unique tool for automated deployment and administration*.

You are free to choose from any of these anti-virus applications, according to the operating systems and applications you use.

## Kaspersky® Anti-Spam

Kaspersky® Anti-Spam is a cutting-edge software suite that is designed to help organizations with small- and medium-sized networks wage war against the onslaught of unsolicited e-mail messages (spam). The product combines the revolutionary technology of linguistic analysis with modern methods of e-mail filtration, including DNS Black Lists and formal letter features. Its unique combination of services allows users to identify and wipe out up to 95% of unwanted traffic.

Installed at the entrance to a network, where it monitors incoming e-mail traffic streams for spam, Kaspersky® Anti-Spam acts as a barrier to unsolicited e-mail. The product is compatible with any mail system and can be installed on either an existing mail server or a dedicated one.

Kaspersky® Anti-Spam's high performance is ensured by daily updates to the content filtration database adding samples provided by the Company's linguistic laboratory specialists. Databases are updated every 20 minutes.

### **Kaspersky® SMTP Gateway**

Kaspersky® SMTP-Gateway for Linux/Unix is a solution designed for anti-virus processing of e-mail transmitted via SMTP. The application contains a number of additional tools for filtering e-mail traffic by name and MIME type of attachments and a number of tools reducing the load on the mail system and preventing hacker attacks. DNS Black List support provides protection against e-mails coming from servers entered in these lists as sources distributing unwanted e-mail (spam).

### **Kaspersky Security® for Microsoft Exchange 2003**

Kaspersky Security for Microsoft Exchange performs anti-virus processing of incoming and outgoing mail messages as well as messages stored at the server, including letters in public folders and filters out unsolicited correspondence using "smart" spam recognition techniques in combination with Microsoft technologies. The application scans all messages arriving at an Exchange Server via SMTP protocol checking them for the presence of viruses using Kaspersky Lab's anti-virus technologies and for the presence of SPAM attributes. It filters out spam based on formal attributes (mail address, IP address, letter size, heading) and analyzes the content of messages and of their attachments using "smart" technologies, including unique graphic signatures for identifying graphic SPAM. The application scans both the message body and the attached files.

### **Kaspersky® Mail Gateway**

Kaspersky Mail Gateway is a comprehensive solution that provides complete protection for users of mail systems. This application installed between the corporate network and the Internet scans all components of e-mail messages for the presence of viruses and other malware (Spyware, Adware, etc.) and performs centralized anti-spam filtration of e-mail stream. This solution also includes some additional mail traffic filtration features.

## **Contact Us**

If you have any questions, comments, or suggestions, please refer them to one of our distributors or directly to Kaspersky Lab. We will be glad to assist you in any matters related to our product by phone or via e-mail. Rest assured that all of your recommendations and suggestions will be thoroughly reviewed and considered.

Technical support	Please find the technical support information at <a href="http://www.kaspersky.com/supportinter.html">http://www.kaspersky.com/supportinter.html</a> Helpdesk: <a href="http://www.kaspersky.com/helpdesk.html">www.kaspersky.com/helpdesk.html</a>
General information	WWW: <a href="http://www.kaspersky.com">http://www.kaspersky.com</a> <a href="http://www.viruslist.com">http://www.viruslist.com</a> E-mail: <a href="mailto:info@kaspersky.com">info@kaspersky.com</a>

---

# APPENDIX C. LICENSE AGREEMENT

## End User License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT") FOR THE LICENSE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY KASPERSKY LAB ("KASPERSKY LAB").

IF YOU HAVE PURCHASED THIS SOFTWARE VIA THE INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE LEGAL ENTITY) CONSENT TO BE BOUND BY AND BECOME PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT, AND DO NOT INSTALL THE SOFTWARE.

IF YOU HAVE PURCHASED THIS SOFTWARE ON A PHYSICAL MEDIUM, HAVING BROKEN THE CD'S SLEEVE YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT BREAK THE CD'S SLEEVE, DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

IN ACCORDANCE WITH THE LEGISLATION, REGARDING KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY ANTI-SPAM PERSONAL, KASPERSKY SECURITY SUITE PERSONAL, KASPERSKY SECURITY FOR PDA) PURCHASED ON LINE FROM THE KASPERSKY LAB INTERNET WEB SITE, CUSTOMER SHALL HAVE A PERIOD OF 7 WORKING DAYS AS FROM THE DELIVERY OF PRODUCT TO MAKE RETURN OF IT TO THE MERCHANT FOR EXCHANGE OR REFUND, PROVIDED THE SOFTWARE IS NOT UNSEALED.

REGARDING THE KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY ANTI-SPAM PERSONAL, KASPERSKY SECURITY SUITE PERSONAL, KASPERSKY SECURITY FOR PDA) NOT PURCHASED ONLINE VIA INTERNET, THIS SOFTWARE NEITHER WILL BE RETURNED NOR EXCHANGED EXCEPT FOR CONTRARY PROVISIONS FROM THE PARTNER WHO SELLS THE

PRODUCT. IN THIS CASE, KASPERSKY LAB WILL NOT BE HELD BY THE PARTNER'S CLAUSES.

THE RIGHT TO RETURN AND REFUND EXTENDS ONLY TO THE ORIGINAL PURCHASER.

All references to "Software" herein shall be deemed to include the software activation key ("Key Identification File") with which you will be provided by Kaspersky Lab as part of the Software.

1. License Grant. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, Kaspersky Lab hereby grants you the non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation") for the term of this Agreement solely for your own internal business purposes. You may install one copy of the Software on one computer, workstation, personal digital assistant, or other electronic device for which the Software was designed (each a "Client Device"). If the Software is licensed as a suite or bundle with more than one specified Software product, this license applies to all such specified Software products, subject to any restrictions or usage terms specified on the applicable price list or product packaging that apply to any such Software products individually.

1.1 Use. The Software is licensed as a single product; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section.

1.1.1 The Software is "in use" on a Client Device when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device. This license authorizes you to make only as many back-up copies of the Software as are necessary for its lawful use and solely for back-up purposes, provided that all such copies contain all of the Software's proprietary notices. You shall maintain records of the number and location of all copies of the Software and Documentation and will take all reasonable precautions to protect the Software from unauthorized copying or use.

1.1.2 If you sell the Client Device on which the Software is installed, you will ensure that all copies of the Software have been previously deleted.

1.1.3 You shall not decompile, reverse engineer, disassemble or otherwise reduce any part of this Software to a humanly readable form nor permit any third party to do so. The interface information necessary to achieve interoperability of the Software with independently created computer programs will be provided by Kaspersky Lab by request on payment of its reasonable costs and expenses for procuring and supplying such information. In the event that Kaspersky Lab notifies you that it does not intend to make such information available for any reason, including (without limitation) costs, you shall be permitted to take such

steps to achieve interoperability, provided that you only reverse engineer or decompile the Software to the extent permitted by law.

1.1.4 You shall not make error corrections to, or otherwise modify, adapt, or translate the Software, nor create derivative works of the Software, nor permit any third party to copy the Software (other than as expressly permitted herein).

1.1.5 You shall not rent, lease or lend the Software to any other person, nor transfer or sub-license your license rights to any other person.

1.1.6 You shall not use this Software in automatic, semi-automatic or manual tools designed to create virus signatures, virus detection routines, any other data or code for detecting malicious code or data.

1.2 Server-Mode Use. You may use the Software on a Client Device or on a server ("Server") within a multi-user or networked environment ("Server-Mode") only if such use is permitted in the applicable price list or product packaging for the Software. A separate license is required for each Client Device or "seat" that may connect to the Server at any time, regardless of whether such licensed Client Devices or seats are concurrently connected to or actually accessing or using the Software. Use of software or hardware that reduces the number of Client Devices or seats directly accessing or utilizing the Software (e.g., "multiplexing" or "pooling" software or hardware) does not reduce the number of licenses required (i.e., the required number of licenses would equal the number of distinct inputs to the multiplexing or pooling software or hardware "front end"). If the number of Client Devices or seats that can connect to the Software exceeds the number of licenses you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits specified for the license you have obtained. This license authorizes you to make or download such copies of the Documentation for each Client Device or seat that is licensed as are necessary for its lawful use, provided that each such copy contains all of the Documentation's proprietary notices.

1.3 Volume Licenses. If the Software is licensed with volume license terms specified in the applicable product invoicing or packaging for the Software, you may make, use or install as many additional copies of the Software on the number of Client Devices as the volume license terms specify. You must have reasonable mechanisms in place to ensure that the number of Client Devices on which the Software has been installed does not exceed the number of licenses you have obtained. This license authorizes you to make or download one copy of the Documentation for each additional copy authorized by the volume license, provided that each such copy contains all of the Document's proprietary notices.

2. Duration. This Agreement is effective for the period specified in the Key File (the unique file which is required to fully enable the Software, please see Help/about Software or Software about, for Unix/Linux version of the Software see the notification about expiration date of the Key File) unless and until earlier terminated as set forth herein. This Agreement will terminate automatically if you fail to comply with any of the conditions, limitations or other requirements

described herein. Upon any termination or expiration of this Agreement, you must immediately destroy all copies of the Software and the Documentation. You may terminate this Agreement at any point by destroying all copies of the Software and the Documentation.

### 3. Support.

(i) Kaspersky Lab will provide you with the support services ("Support Services") as defined below for a period of one year following:

(a) Payment of its then current support charge, and:

(b) Successful completion of the Support Services Subscription Form as provided to you with this Agreement or as available on the Kaspersky Lab website, which will require you to produce the Key Identification File which will have been provided to you by Kaspersky Lab with this Agreement. It shall be at the absolute discretion of Kaspersky Lab whether or not you have satisfied this condition for the provision of Support Services.

(ii) Support Services will terminate unless renewed annually by payment of the then-current annual support charge and by successful completion of the Support Services Subscription Form again.

(iii) By completion of the Support Services Subscription Form you consent to the terms of the Kaspersky Lab Privacy Policy, which is deposited on [www.kaspersky.com/privacy](http://www.kaspersky.com/privacy), and you explicitly consent to the transfer of data to other countries outside your own as set out in the Privacy Policy.

(iv) "Support Services" means:

(a) Daily updates of the anti-virus database;

(b) Free software updates, including version upgrades;

(c) Extended technical support via e-mail and phone hotline provided by Vendor and/or Reseller;

(d) Virus detection and disinfection updates 24 hours per day.

4. Ownership Rights. The Software is protected by copyright laws. Kaspersky Lab and its suppliers own and retain all rights, titles and interests in and to the Software, including all copyrights, patents, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer any title to the intellectual property in the Software to you, and you will not acquire any rights to the Software except as expressly set forth in this Agreement.

5. Confidentiality. You agree that the Software and the Documentation, including the specific design and structure of individual programs and the Key Identification File, constitute confidential proprietary information of Kaspersky Lab. You shall not disclose, provide, or otherwise make available such confidential information in any form to any third party without the prior written consent of Kaspersky Lab.

You shall implement reasonable security measures to protect such confidential information, but without limitation to the foregoing shall use best endeavours to maintain the security of the Key Identification File.

#### 6. Limited Warranty.

(i) Kaspersky Lab warrants that for six (6) months from first download or installation the Software purchased on a physical medium will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.

(ii) You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Lab does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted or error free.

(iii) Kaspersky Lab does not warrant that this Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.

(iv) Your sole remedy and the entire liability of Kaspersky Lab for breach of the warranty at paragraph (i) will be at Kaspersky Lab option, to repair, replace or refund of the Software if reported to Kaspersky Lab or its designee during the warranty period. You shall provide all information as may be reasonably necessary to assist the Supplier in resolving the defective item.

(v) The warranty in (i) shall not apply if you (a) make or cause to be made any modifications to this Software without the consent of Kaspersky Lab, (b) use the Software in a manner for which it was not intended, or (c) use the Software other than as permitted under this Agreement.

(vi) The warranties and conditions stated in this Agreement are in lieu of all other conditions, warranties or other terms concerning the supply or purported supply of, failure to supply or delay in supplying the Software or the Documentation which might but for this paragraph (vi) have effect between the Kaspersky Lab and you or would otherwise be implied into or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded (including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or as to the use of reasonable skill and care).

#### 7. Limitation of Liability.

(i) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for (a) the tort of deceit, (b) death or personal injury caused by its breach of a common law duty of care or any negligent breach of a term of this Agreement, or (c) any other liability which cannot be excluded by law.

(ii) Subject to paragraph (i) above, the Supplier shall bear no liability (whether in contract, tort, restitution or otherwise) for any of the following losses or damage

(whether such losses or damage were foreseen, foreseeable, known or otherwise):

- (a) Loss of revenue;
- (b) Loss of actual or anticipated profits (including for loss of profits on contracts);
- (c) Loss of the use of money;
- (d) Loss of anticipated savings;
- (e) Loss of business;
- (f) Loss of opportunity;
- (g) Loss of goodwill;
- (h) Loss of reputation;
- (i) Loss of, damage to or corruption of data, or:
- (j) Any indirect or consequential loss or damage howsoever caused (including, for the avoidance of doubt, where such loss or damage is of the type specified in paragraphs (ii), (a) to (ii), (i).
- (iii) Subject to paragraph (i), the liability of Kaspersky Lab (whether in contract, tort, restitution or otherwise) arising out of or in connection with the supply of the Software shall in no circumstances exceed a sum equal to the amount equally paid by you for the Software.

8. (i) This Agreement contains the entire understanding between the parties with respect to the subject matter hereof and supersedes all and any prior understandings, undertakings and promises between you and Kaspersky Lab, whether oral or in writing, which have been given or may be implied from anything written or said in negotiations between us or our representatives prior to this Agreement and all prior agreements between the parties relating to the matters aforesaid shall cease to have effect as from the Effective Date. Save as provided in paragraphs (ii) - (iii) below, you shall not have any remedy in respect of an untrue statement made to you upon which you relied in entering into this Agreement ("Misrepresentation") and Kaspersky Lab shall not have any liability to the other than pursuant to the express terms of this Agreement.

(ii) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for any Misrepresentation made thereby if aware that it was untrue.

(iii) The liability of Kaspersky Lab for Misrepresentation as a fundamental matter, including a matter fundamental to the maker's ability to perform its obligations under this Agreement, shall be subject to the limitation of liability set out in paragraph 7(iii).