



## Kaspersky Hosted Security Terms&Conditions

These Terms&Conditions (T&Cs) shall govern the provision of Kaspersky Hosted Security (KHS) by Kaspersky Lab to the Customer.

### 1 Definitions and Interpretations

In these T&Cs the following words shall have the following meaning:

**Customer:** means the company or other legal entity to which the KHS is provided.

**Kaspersky Lab:** means for the purposes of this Schedule the Kaspersky Group.

**Kaspersky Hosted Email Security:** means the Kaspersky Hosted Email Security as described in the most recent version of the KHS Description.

**Kaspersky Hosted Web Security:** means the Kaspersky Hosted Web Security as described in the most recent version of the KHS Description.

**Kaspersky Hosted Security (KHS)** means the Kaspersky Hosted Email Security and/or the Kaspersky Hosted Web Security or any combination thereof, as described in the most recent version of the KHS Description.

**KHS Description:** means provisions in which technical descriptions of the KHS are contained and the most recent version of which is attached to these T&Cs.

**Malware:** means a computer program written with an explicit intent of harming or compromising data and/or code on a targeted computer, and/or reducing its usability, and/or enabling unauthorized access to it.

**Monthly Charge** means 1/12 of the price paid by the Customer for one year of the KHS usage, or the price paid by the Customer for one month of the KHS usage.

**Open Relay:** means an SMTP server configured in such a way that it allows anyone on the Internet to send e-mail through it, not just mail destined to or originating from known users or domains.

**Permitted Number of Users:** means the number of Users set out in the License Certificate.

**Portal:** means a web-based configuration that is used by the Customer for management of the KHS and reporting.

**License Certificate** means the certificate confirming the KHS license grant, subscription period and permitted number of users, to which these T&Cs are attached.

**Subscription Period** means the period paid by the Customer during which the Customer uses KHS as set out in the License Certificate.

**Start Date:** means KHS activation date set out in the License Certificate.

**Spam and E-mail Spam:** mean unsolicited bulk messages sent indiscriminately.

**User** means (i) a physical or virtual (for the cases of shared mailboxes) entity who has 1 corporate mailbox with one or more related aliases for it, and for whom the Kaspersky Hosted Email Security scans e-mails and/or (ii) a physical or virtual (for the cases of shared computers) entity who can access Internet resources and for whom the Kaspersky Hosted Web Security processes Web Content.

**Web Content** means any data and requests for data processed by the Kaspersky Hosted Web Security including but not restricted to that accessed using the Internet protocols HTTP and FTP.

### 2 Scope of application of these T&Cs

2.1 Kaspersky Lab grants to the Customer rights to use the KHS according to the terms and conditions provided herein.

2.2 These T&Cs shall apply for the provision of the KHS by Kaspersky Lab. The Schedules and the Appendices thereto shall apply insofar as the part of KHS described therein is indicated in the License Certificate. Any and all deviating T&Cs stated on the Customer's order or in any other Customer documents are rejected and shall be null and void unless expressly agreed to in writing by both parties.

### 3 Duration

3.1 These T&Cs shall commence on the Start Date and subject to Clause 4 shall continue in force for the Subscription Period.

#### **4 Termination**

- 4.1 Kaspersky Lab shall be entitled to terminate the T&Cs with immediate effect by notification to the Customer in the event that the Customer fails to pay for the KHS in accordance with the relevant terms;
  - 4.1.1 Kaspersky Lab will monitor the usage of the KHS by the Customer. If the actual number of Users exceed the Permitted Number of Users Kaspersky Lab shall be entitled in its sole discretion either to terminate the T&Cs with immediate effect by notification to the Customer or to make a commensurate and immediately payable charge for the additional number of Users.
- 4.2 Without prejudice to any other rights to which it may be entitled under these T&Cs, either party may terminate the T&Cs with immediate effect by giving written notice to the other if the other party commits a material breach of these T&Cs and (if such a breach is capable of remedy) fails to remedy the breach within thirty (30) days after being required by written notice to do so.
- 4.3 Upon termination by the Customer under Clause 4.2 for breach of these T&Cs by Kaspersky Lab, the proportion of fees paid by the Customer that relates to the Subscription period not used post termination shall be refunded to the Customer.
- 4.4 Upon termination of the T&Cs as a result of the Customer's breach of these T&Cs the Customer's right to use the KHS shall cease with immediate effect and all invoices shall become due and payable.
- 4.5 The following clauses of these T&Cs shall survive termination: Clauses 1, 7, 8, 9, 10, 13, 14 and 20.

#### **5 KHS Provision**

- 5.1 Kaspersky Lab undertakes to use all reasonable endeavours to provide the KHS for the Permitted Number of Users for the Subscription Period.
- 5.2 Kaspersky Lab reserves the right both prior to the enrolment of the Kaspersky Hosted Email Security and at any time during the supply of the Kaspersky Hosted Email Security to test whether the Customer's email system is acting as an Open Relay. If the Customer's systems are found to be acting as an Open Relay, Kaspersky Lab will inform the Customer and reserves the right to suspend all or part of the Kaspersky Hosted Email Security immediately until the problem has been resolved.
- 5.3 If at any time provision of the KHS to the Customer would compromise the security of the KHS due, but not limited to, hacking, denial of service attacks, flooding or other malicious activities originating from or directed at the Customer's network, Kaspersky Lab reserves the right to suspend all or part of the KHS immediately and until the problem has been resolved. In such an event, Kaspersky Lab will promptly inform the Customer and work with the Customer, who is obliged to co-operate, to resolve such issues in order to reinstate the KHS at the earliest possible opportunity.
- 5.4 If at any time the Customer is using the Kaspersky Hosted Email Security to distribute Spam, Kaspersky Lab reserves the right to suspend all or part of Kaspersky Hosted Email Security immediately and until the problem has been solved.
- 5.5 Should the KHS be suspended or terminated for any reason whatsoever, Kaspersky Lab shall reverse all configuration changes made on enrolment to the KHS and it shall be the responsibility of the Customer to undertake all other necessary configuration changes in order to correctly reroute its email and/or web traffic.
- 5.6 Subject to applicable legislation, Kaspersky Lab may provide the KHS using any hardware installation anywhere in the world and may, at any time, transfer the provision of the KHS from one installation to another.
- 5.7 In order to fulfill its obligations, Kaspersky Lab may amend the KHS and any documentation relating thereto from time to time for any reason including, but not limited to, changes in line with industry standards as well as any legal, business or technical considerations. Any change will be effective upon Kaspersky Lab publishing a new KHS Description on the Portal.

#### **6 Customer Obligations**

- 6.1 The Customer acknowledges that the KHS will be provisioned with Kaspersky Lab standard settings applied by default and that it is the Customer's sole responsibility to configure the KHS by the mean of Portal to satisfy its own requirements. Kaspersky Lab representatives may help with configuring the KHS in a way that is optimal for its running. Kaspersky Lab reserves the right to change customer settings in emergency situations to preserve the KHS quality for one or more Customers.
- 6.2 The Customer will provide Kaspersky Lab with all technical data and all other information Kaspersky Lab may reasonably request from time to time to allow Kaspersky Lab to supply the KHS to the Customer. All information the Customer supplies will be complete, accurate and given in good faith. Such information will be treated as Confidential Information under the terms and conditions of these T&Cs.
- 6.3 The Customer shall not allow its Email system to:
  - 6.3.1 act as an Open Relay;
  - 6.3.2 send Spam.
- 6.4 The Customer recognises that information sent to and from the Customer will pass through the KHS and accordingly the Customer agrees to:
  - 6.4.1 comply with all relevant legislation applicable to the use of the Internet and emails;
  - 6.4.2 use the KHS for legitimate business purposes only, which includes the sending and receiving of business and personal emails / use of Web-Content by its employees;
  - 6.4.3 not use the KHS for the transition of Spam;
  - 6.4.4 comply with the protocols and standards published on the Internet from time to time and adopted by the majority of



Internet users;

- 6.4.5 indemnify Kaspersky Lab against any liability to third parties resulting from information passing through the KHS from the Customer.
- 6.5 The Customer agrees not to use the KHS for any unlawful purpose and to indemnify Kaspersky Lab against all and any losses, costs and expenses which Kaspersky Lab may incur by such unlawful activities, including but not limited to:
- 6.5.1 civil or criminal offences of Intellectual property rights infringement, including, but not limited to copyright, trade mark and patent infringement; or
  - 6.5.2 transmission or posting of obscene, indecent or pornographic materials; or
  - 6.5.3 carrying out any criminal offence under the relevant legislation; or
  - 6.5.4 transmission or posting of any material which is defamatory, offensive, abusive, or menacing, or
  - 6.5.5 transmission or posting of any material in breach of the Data Protection Act 1998 or any similar applicable legislation;
  - 6.5.6 use of the KHS in any manner which violates or infringes the rights of any individual, organisation or company.
- 6.6 The Customer is only permitted to add email domains that the Customer owns or has a legal proof that he is entitled to add the domain to the Kaspersky Hosted Security system. Kaspersky Lab reserves the right to verify domain ownership or entitlement before commissioning of the KHS.
- 6.7 For the avoidance of doubt, any breach of Clauses 6.3-6.6 inclusive will constitute a material breach of the T&Cs. In the event the Customer does not comply with any obligations set out in Clauses 6.3-6.6, then without prejudice to its other rights in the T&Cs or the Agreement Kaspersky Lab may at any time suspend the usage of the KHS by the Customer until the Customer has resolved the problem.
- 6.8 The KHS is provided to the Customer for its own use and the Customer shall not resell it to any third party.

## 7 Warranty

Kaspersky Lab will use all reasonable professional skill and care necessary to provide the KHS to the extent permitted by law. The foregoing conditions are in lieu of and exclude all other express and implied warranties, conditions and other terms, including but not limited to warranties of satisfactory quality and fitness for a particular purpose.

## 8 Limitation of Liability

ANY SUBSTANTIATED LAWFUL CLAIMS OF THE CUSTOMER RELATED TO THE AVAILABILITY AND/OR THE QUALITY OF THE KHS AS WELL AS ANY OTHER CLAIMS IN CONNECTION WITH THE KHS ARE SUBJECT TO THE FOLLOWING LIMITATIONS:

- 8.1 KASPERSKY LAB'S LIABILITY FOR ACTUAL LOSS AND DAMAGES BY THE CUSTOMER (INCLUDING LOSS OF DATA) OR CLAIMS OF THIRD PARTIES THAT MIGHT BE DERIVED FROM THE CUSTOMER'S CLAIMS CAUSED BY NON-COMPLIANCE OF THE KHS WITH THE KHS DESCRIPTION (E.G. UNAVAILABILITY, DEFECTS OR QUALITY OF THE KHS) CAUSED BY NEGLIGENCE OF KASPERSKY LAB, ITS EMPLOYEES OR ITS AGENTS SHALL BE LIMITED TO A MAXIMUM OF THE MOST RECENT ACTUAL AMOUNT TO BE PAID BY THE CUSTOMER FOR THE KHS FOR A PERIOD OF ONE (1) YEAR. SUCH LIMIT SHALL APPLY TO EACH EVENT OR SERIES OF CONNECTED EVENTS.
- 8.2 ANY CLAIMS OF THE CUSTOMER FOR THE REIMBURSEMENT OF A LOSS OF PROFIT / LOSS OF SALE / LOSS OF REPUTATION / LOSS OF CONTRACTS AND/OR CUSTOMERS OR COMPENSATION FOR LOSS OF DATA ARE EXCLUDED.
- 8.3 KASPERSKY LAB SHALL NOT BE LIABLE FOR DAMAGES CAUSED BY CUSTOMER BY NON-COMPLIANCE WITH THE T&CS, OR BY USING THE KHS IN A WAY NOT COMPLYING WITH THE T&CS.
- 8.4 THE ABOVE LIMITATIONS AND EXCLUSIONS DO NOT APPLY IN CASE OF:
- 8.4.1 THE DEATH OF, OR PERSONAL INJURY TO, ANY PERSON OR ANY PERSON'S HEALTH,
  - 8.4.2 ANY LIABILITY WHICH CANNOT BE LIMITED OR EXCLUDED BY LAW,
  - 8.4.3 THE INTELLECTUAL PROPERTY RIGHTS INDEMNITY SPECIFIED IN CLAUSE 14.
- 8.5 **THE CUSTOMER'S PARTICULAR ATTENTION IS DRAWN TO THE FACT THAT THE KHS IS PROVIDED BY THE USE OF ELECTRONIC MEASURES AND ALGORITHMS AS DESCRIBED IN THE T&CS AND IN THE KHS DESCRIPTION:**
- 8.5.1 HAVING REGARD TO THE STATE OF TECHNOLOGICAL DEVELOPMENT THESE MEASURES WILL BE MAINTAINED BY KASPERSKY LAB AT A REASONABLE LEVEL TO ENSURE THAT NORMALLY ONLY EMAILS THAT CONTAIN VIRUSES OR ARE TO BE REGARDED AS SPAM ARE DETECTED AS "POSITIVE" AND THEREFORE MAY BE BLOCKED AND QUARANTINED ACCORDING TO THE PROVISIONS SET OUT IN THESE T&CS AND IN THE KHS DESCRIPTION. HOWEVER, IT IS NOT POSSIBLE TO ENSURE THAT IN CERTAIN CASES AND UNDER CERTAIN CIRCUMSTANCES (WHICH MAY INCLUDE THE CUSTOMER'S CONFIGURATION) WANTED OR NOT VIRUS-INFECTED EMAILS WILL ALSO BE BLOCKED AND QUARANTINED ("FALSE POSITIVE"). THEREFORE THE CUSTOMER



ACCEPTS THE OBLIGATION TO CHECK THE QUARANTINE BOX OF THE KHS AT REGULAR INTERVALS. KASPERSKY LAB DOES NOT ACCEPT ANY LIABILITY FOR ANY LOSS AND/OR DAMAGES RESULTING FROM THE NON-DELIVERY OF FALSE POSITIVE EMAILS AND FURTHER KASPERSKY LAB DOES NOT ACCEPT ANY LIABILITY IN THE EVENT THAT ANY "FALSE POSITIVE" MAILS HAVE BEEN DELETED AFTER THE 30 DAYS FROM THE DATE ON WHICH THEY WERE SENT.

## **9 Confidentiality**

- 9.1 Each party agrees and undertakes that during the term of the Subscription Period and for three (3) years thereafter it will (subject to Clauses 9.2 and 9.3) keep confidential and will not use for its own purposes nor, without the prior written consent of the other party, disclose to any third party any information of a confidential nature (including trade secrets and information of commercial value) which may have been disclosed to or become known to that party through the other party or its subcontractors ("Confidential Information"). Undertakings regarding Confidential Information shall not apply where the information is public knowledge or where a party can prove the information was already known to it at the time of disclosure or where it subsequently becomes public knowledge other than by breach of these T&Cs or where it is subsequently lawfully obtained from a third party without any obligation of confidence. Neither party nor any of its subcontractors shall be deemed to be in breach of this Clause where it is required by law to disclose Confidential Information, provided that it has first given the other party a minimum of 14 days' notice of the legal requirement to disclose.
- 9.2 To the extent necessary to implement and/or to comply with the provisions of these T&Cs each party may disclose the Confidential Information to those of its employees and subcontractors who have a need to know the Confidential Information for such purposes provided that before any such disclosure each party shall make those employees and subcontractors aware of its obligations of confidentiality under these T&Cs and shall procure compliance by those employees and subcontractors.
- 9.3 Kaspersky Lab recognises that the content of all emails sent to or received from the Customer and all Customer Web Content and requests for Web Content are confidential. Kaspersky Lab will, other than in compliance of its contractual obligations, neither inspect nor use the content of Customer's emails, Web Content or requests for Web Content. In the normal provision of the KHS Kaspersky Lab will not access, read and/or copy emails and/or their attachments, Web-Content and requests for Web Content other than for the purposes of providing the KHS. Any data will be treated as strictly confidential.
- 9.4 However, Kaspersky Lab reserves the right to utilise the Virus-related content of such email and/or its attachments / of Web-Content and the data of the Internet connection used by the Customer solely for the purposes of:
- 9.4.1 maintaining and improving the performance and the integrity of the KHS,
  - 9.4.2 complying with all regulatory, legislative or contractual requirements, and
  - 9.4.3 making the Virus-related content available to licensors of the KHS for the purpose of further developing and enhancing the KHS.
- 9.5 Further Kaspersky Lab reserves the right to utilise the Spam-related content of such email and/or its attachments sent to the Customer's domain, for which no Email-address is configured on the Customer's server, solely for the purposes of:
- 9.5.1 maintaining and improving the performance and the integrity of the KHS,
  - 9.5.2 complying with all regulatory, legislative or contractual requirements, and
  - 9.5.3 making the Spam-related content available to licensors of the KHS for the purpose of further developing and enhancing the KHS.

## **10 Data Privacy and Regulation of Investigatory Powers**

- 10.1 The Customer shall take all necessary measures to ensure that it, and all its employees, are aware of their responsibilities in respect of all applicable data protection laws and/or regulations and, as Kaspersky Lab has no control or influence over the content of the emails/ the Web Content processed by the KHS, the Customer shall hold Kaspersky Lab harmless and fully indemnified for any claims by any party relating to any breach of the Data Protection Act 1998 or any similar applicable legislation by the Customer.
- 10.2 The Customer shall procure any consent and give any indication required in connection with processing, storing and using of personal data necessary for providing KHS according to these T&Cs.
- 10.3 To the extent that in providing KHS personal data are processed, this is done exclusively in compliance with the provisions of these T&Cs and only for the purposes and to the extent necessary for providing KHS.
- 10.4 The Customer warrants that it has complied with all applicable rules and regulations in connection with the implementation of an email/Internet policy within its organisation and, if relevant, has obtained the consent of its employees or works council as to the KHS, in particular, intercepting, reading, copying or filtering emails and/or their attachments/ Web-content.
- 10.5 As required by any applicable law, the Customer shall inform (for example via a banner message on emails) those who use any communications system covered by the KHS, that communications transmitted through such system may be intercepted and monitored, and indicate the purposes of such interception and monitoring. Neither party shall use, nor require the other party to use, any data obtained via the KHS for any unlawful purposes.

## **11 Force Majeure**

The obligations of each party under these T&Cs shall be suspended during the period and to the extent that such party is unavoidably prevented or hindered from complying with them by any cause beyond its reasonable control including events



such as, but not limited to: strikes, lock-outs, war, terrorism, riot, civil commotion, malicious damage, compliance with any law or governmental order, regulation or direction, accident, fire, flood, storm, power outages or failures of essential third party service systems or connections.

## **12 Suspension**

Any suspension of the KHS permitted by these T&Cs, other than due to Kaspersky Lab's default, shall not extend the Subscription period.

## **13 Intellectual Property Rights**

The Customer agrees that the KHS and the authorship, systems, ideas, methods of operation, documentation and other information contained in the KHS, are proprietary intellectual property and/or the valuable trade secrets of the Kaspersky Lab or its partners and that the Kaspersky Lab and its partners, as applicable, are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patent of the Russian Federation, European Union and the United States of America, as well as other countries and international treaties. These T&Cs do not grant to the Customer any rights to the said intellectual property including any the Trademarks or Service Marks of the Kaspersky Lab and/or its partners ("Trademarks"). Permitted use of any Trademark does not give the Customer any rights of ownership in that Trademark. The Rightholder and/or its partners own and retain all right, title, and interest in and to the KHS, including without limitation any error corrections, enhancements, Updates or other modifications to the KHS, whether made by the Kaspersky Lab or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. The Customer's use of the KHS does not transfer to the Customer any title to the intellectual property in the KHS, and the Customer will not acquire any rights to the KHS except as expressly set forth in these T&Cs. Except as stated herein, these T&Cs do not grant the Customer any intellectual property rights in the KHS and the Customer acknowledges that the KHS product license, as further defined herein, granted under these T&Cs only provides the Customer with a right of use of KHS under these T&Cs for a limited period. Kaspersky Lab reserves all rights not expressly granted to the Customer in these T&Cs.

## **14 Third Party Intellectual Property Rights**

14.1 In the event that the KHS infringes any third party intellectual property rights, Kaspersky Lab will defend and/or settle any third party claim provided that:

14.1.1 the Customer promptly on becoming aware of the same, notifies Kaspersky Lab of any such claim in writing;

14.1.2 the Customer gives Kaspersky Lab the sole control of any such action or proceedings;

14.1.3 the Customer fully co-operates with Kaspersky Lab and provides such assistance as it may reasonably require to settle and/or defend such action or proceedings (at the cost of Kaspersky Lab);

14.1.4 any award of costs and/or damages shall belong to Kaspersky Lab.

14.2 In the event that KHS infringes any third party intellectual property rights, Kaspersky Lab at its sole option shall replace KHS with a non-infringing product, or may terminate the T&Cs forthwith by written notice to the Customer in which case any claims for compensation of damages shall be excluded but Customer shall be entitled to a refund for that proportion of the fees paid which relate to the remainder of the Subscription Period.

14.3 The provisions of Clause 14.1 and 14.2 above shall not apply to any infringement resulting from:

14.3.1 the use of the KHS which does not comply with the uses permitted under these T&Cs; or

14.3.2 the combination of the KHS with any third party product and/or service or modification undertaken by the Customer without the prior written consent of Kaspersky Lab, if such combination or modification causes the infringement.

## **15 Publicity**

The Customer and Kaspersky Lab agree that each party may disclose that they share a business relationship. Kaspersky Lab is in particular entitled to include the Customer in its Customer reference list. But further details of the business relationship and any details of the Agreement or these T&Cs shall not be disclosed without the express consent of the other party.

## **16 Amendments**

16.1 Neither an amendment or variation nor the cancellation of these T&Cs shall be effective unless in writing. This includes the amendment or cancellation of this clause itself.

16.2 Notwithstanding Clause 16.1 Kaspersky Lab reserves the right to modify technical details of the KHS, as long as the quality of the KHS is not impaired. Should such modification for bona fide reasons be unacceptable to the Customer, both parties shall have the right to terminate the T&Cs with immediate effect. Any claims for compensation of damages shall be excluded in this case but Customer shall be entitled to a refund for that proportion of the fees paid which relate to the remainder of the Subscription Period.

## **17 Assignment**

Customer is not entitled to assign these T&Cs or claims hereunder without Kaspersky Lab's prior written consent.



**18 Severability**

If any provision of these T&Cs is or becomes null and void, the remainder of these T&Cs shall continue in full force and effect. The parties in this case undertake to replace the provision null and void by another valid provision corresponding most closely to the provision null and void, and to the objective of the contract.

**19 Schedules**

The KHS Description and Schedules attached hereto shall be a substantial part of these T&Cs.

**20 Governing Law and Jurisdiction**

- 20.1 This T&Cs shall be governed by and construed in accordance with applicable laws of a country where the KHS was acquired.
- 20.2 The parties irrevocably agree that the courts of England have non-exclusive jurisdiction to settle any dispute or claim that arises out of or in connection with these T&Cs.



# Kaspersky Hosted Security Description

## 1 Summary

Kaspersky Lab is a company that specializes in IT-Security products. We offer Kaspersky Hosted Security (KHS) to enforce companies' IT-Security policies. The KHS is available for email (Kaspersky Hosted Email Security) and web (Kaspersky Hosted Web Security). This document describes all parts of KHS regardless of which parts of the product suite are licensed.

This KHS Description shall only be applicable insofar as the Customer has purchased licenses for the respective part of KHS and under the terms and conditions of the T&Cs to which this KHS Description is attached. Words capitalized but not defined in this KHS Description will have the meaning defined in the T&Cs.

## 2 Definitions

- 2.1 **Designated Cluster** means a cluster of servers, designated to provide the KHS to the Customer on a non-exclusive basis.
- 2.2 **Normal Working Day** means Monday to Friday excluding public holidays as recognized Kaspersky Lab's domicile.
- 2.3 **Out of Hours** means any time other than Working Hours.
- 2.4 **Guarantees** means collectively the parameters of KHS work defined in this KHS Description.
- 2.5 **Working Hours** means business hours of each Normal Working Day.

## 3 Availability of KHS

- 3.1 The KHS is available on a twenty-four (24) hours/day by seven (7) days/week basis from Kaspersky Lab's Operations Centers. The KHS is monitored for availability, capacity and network resource utilization. Through stringent monitoring regular adjustments are made to the KHS to ensure optimum efficiency is maintained.
- 3.2 The KHS is highly available and scalable. All traffic is load-balanced between data centers in different geographical areas. Each data center itself is built in a highly available manner to provide maximum uptime. In the unlikely event of a complete data centre failure the backup data centre for the Customer will assume responsibility with no noticeable disruption to traffic flow.
- 3.3 The Guarantees will NOT apply:
  - 3.3.1 if Customer is using the KHS to distribute Spam;
  - 3.3.2 if the Customer's email system is acting as Open Relay;
  - 3.3.3 unless the Customer is utilizing the Designated Cluster technology;
  - 3.3.4 during the Trial period ;
  - 3.3.5 if the Customer's system configuration is not compliant with all Kaspersky Lab's standard configuration guidelines as published from time to time;
  - 3.3.6 during periods of Planned Maintenance (subject to Clause 4), periods of non-availability due to force majeure or acts or omissions of either the Customer or a third party;
  - 3.3.7 during any period of suspension of KHS by Kaspersky Lab in accordance with the T&Cs;
  - 3.3.8 failure of the Customers infrastructure or internet connection;
  - 3.3.9 KHS unavailability caused by incorrect information supplied by the Customer;
  - 3.3.10 reasons out of Kaspersky Lab's reasonable control as defined in the T&Cs.

## 4 Planned Maintenance

- 4.1 Planned Maintenance means periods of maintenance which may cause disruption of KHS due to non availability of Cluster(s) or their parts. Wherever possible, planned maintenance will be carried out without affecting the KHS. This will generally be achieved by carrying out planned maintenance during periods of anticipated low email traffic and by carrying out planned maintenance in such stages designed to avoid any detrimental effect on Customers. During planned maintenance periods the traffic may be diverted round sections of the network not undergoing maintenance in order to minimize disruption to the KHS.
- 4.2 Planned Maintenance shall not take place between 8am and 6pm (in the time zone in which a cluster is located).
- 4.3 The Customer will be notified about the Planned Maintenance by Kaspersky Lab not less than seven (7) days prior to the Planned Maintenance. Kaspersky Lab may inform the Customer by sending email and/or may post an alert message on Portal.
- 4.4 Where emergency maintenance is necessary and is likely to affect the KHS, Kaspersky Lab will endeavour to inform the Customer and may post an alert message on Portal.

## 5 Web Portal



- 5.1 An integral part of the KHS is a web-based configuration, management and reporting tool referred to as the Portal. After a Customer has enrolled on the KHS, a unique user name and password is created to give Customer's administrator full access to the Customer's Portal account where policies and settings can be configured. The Portal also gives access to statistics, reporting and quarantined emails.
- 5.2 The Portal is available in English, French, German and Russian languages.

## 6 Technical Support

- 6.1 Kaspersky Lab will provide technical support on a twenty-four (24) hours/day by seven (7) days/week basis. Support calls can be raised by telephone or email.
- 6.2 During Working Hours, support is available in English, French, German and Russian languages. Out of Hours support is available in English language.
- 6.3 Kaspersky Lab aims and will use its reasonable efforts to answer all telephone calls within 60 seconds and start work on a case within 1 hour.
- 6.4 Customers will receive a ticket number for each support call.
- 6.5 Contact Details:

	E-mail address	Telephone number
Benelux (Dutch and English)	<a href="mailto:KHS-Support@kaspersky.com">KHS-Support@kaspersky.com</a>	+31(0)307529539
Denmark, Finland, Norway, Sweden (Swedish, Danish, Norwegian, Finnish, English)	<a href="mailto:KHS-Support@kaspersky.com">KHS-Support@kaspersky.com</a>	+46(0)85 785 3031
Germany, Austria, Switzerland (German)	<a href="mailto:KHS-Support@kaspersky.com">KHS-Support@kaspersky.com</a>	+49(0)84198189760
France (French)	<a href="mailto:KHS-Support@kaspersky.com">KHS-Support@kaspersky.com</a>	+33(0)141398933
Italy	<a href="mailto:KHS-Support@kaspersky.com">KHS-Support@kaspersky.com</a>	+39(06)58891091
Russia (Russian)	<a href="mailto:KHS-Support@kaspersky.com">KHS-Support@kaspersky.com</a>	+7 (495) 9567800
Spain (Spanish)	<a href="mailto:KHS-Support@kaspersky.com">KHS-Support@kaspersky.com</a>	+34 913983566
UK (English)	<a href="mailto:KHS-Support@kaspersky.com">KHS-Support@kaspersky.com</a>	+44(0)8454590165
Australia (English)	<a href="mailto:KHS-Support@kaspersky.com">KHS-Support@kaspersky.com</a>	1300 268 484 +61(3)96230414
New Zealand (English)	<a href="mailto:KHS-Support@kaspersky.com">KHS-Support@kaspersky.com</a>	0800 268 484
Malaysia, Philippines, Singapore (English, Malay, Chinese)	<a href="mailto:KHS-Support@kaspersky.com">KHS-Support@kaspersky.com</a>	+60(3)79625930
Other countries (English)	<a href="mailto:KHS-Support@kaspersky.com">KHS-Support@kaspersky.com</a>	+7 (495) 9567800

- 6.6 All incoming support calls will be logged and prioritized in accordance with the following matrix:

Priority	Problem	Response during Working Hours	Response Out of Hours	Resolution
I	KHS unavailable or major incident	1 hour	1 hour	As soon as reasonably possible but in all circumstance within 24 hours
II	Partial loss of KHS but traffic is still processed	2 hours	12 hours	As soon as reasonably possible but with best efforts to achieve resolution within two Normal Working Days
III	Technical or configuration problems	4 hours	Next working day	Agreement between Customer and Support Team
IV	Standard questions, quarantine support, information issues	1 Normal Working day	Next working day	Agreement between Customer and Support Team



## 7 Credit Requests

- 7.1 In the event that the Customer believes they are entitled to a compensation in accordance with this KHS Description, the Customer must submit a Credit Request. "Credit Request" means the notification which the Customer must submit to [KHS-Support@kaspersky.com](mailto:KHS-Support@kaspersky.com) with the subject line "Credit Request" (unless otherwise notified by Kaspersky Lab) within the time limit specified in the KHS Description. Subject to verification of such entitlement by Kaspersky Lab, Kaspersky Lab will credit the Customer in accordance with the appropriate provisions of this KHS Description. There is no refunds of fees paid. THE CUSTOMER RECOGNIZES THAT LOGS ARE ONLY KEPT FOR A LIMITED NUMBER OF DAYS AND THEREFORE ANY CREDIT REQUEST SUBMITTED OUTSIDE OF THE PROVIDED TIMEFRAME WILL BE DEEMED INVALID AND THEREFORE THE CUSTOMER HAS NO RIGHT TO THE CREDIT.



## Kaspersky Hosted Email Security

### 8 Definitions

- 8.1 **False Negative** means a Spam and/or a Malware infected email that is not identified as Spam and/or Malware;
- 8.2 **False Positive** means a legitimate email incorrectly marked/captured as Spam and/or Malware.
- 8.3 **Known Malware** means the Malware which has already been identified, and for which a signature or definition has been made available which when applied to traffic will detect the Malware, by either Kaspersky Lab or one of Kaspersky Lab's technology partners whose anti-malware technology is used in Kaspersky Hosted Email Security, at least twenty (20) minutes prior to the KHS scanning an email infected by such Malware.

### 9 Overview

- 9.1 The Kaspersky Hosted Email Security provides Anti-Spam and Anti-Malware scanning of emails and attachments to determine whether they contain Malware or Spam. Both inbound and outbound email filtering is provided.
- 9.2 The Kaspersky Hosted Email Security is available to Customers whose email systems are permanently connected to the Internet with a fixed IP address. It cannot be provided to Customers whose email systems are connected to the Internet via dial-up or ISDN lines or whose IP address is dynamically allocated.
- 9.3 All email traffic will be routed using SMTP through a Designated Cluster.
- 9.4 Kaspersky Lab offers an opportunistic encrypted link between the assigned data centre and the mail server of the Customer using TLS (if the Customer's mail server supports TLS encryption).
- 9.5 Kaspersky Hosted Email Security will scan emails up to a maximum size of 100MB. Emails greater than 100MB will be rejected with an appropriate error code.
- 9.6 For all incoming mails the IP reputation of the sender is ascertained. Email originating from a disreputable source (such as a spammer) will be slowed down or rejected at the connection layer to minimize KHS impact.
- 9.7 The Customer can add email domains to the Portal for the purpose of filtering emails.
- 9.8 Kaspersky Hosted Email Security offers various options for user handling. The Customer can define whether it accepts: all email addresses for a domain added automatically; only manually defined email addresses; only email addresses confirmed as valid using SMTP authorization; only email addresses confirmed as valid by the Service making an LDAP call to the Customer's directory server.

### 10 Kaspersky Hosted Email Security. Anti-Spam

- 10.1 The anti-spam functionality uses multiple technologies to ensure highest spam detection rates.
- 10.2 The anti-spam engine is continuously tuned to identify emails which are almost certainly spam ("Spam") and those likely to be spam ("Probable Spam").
- 10.3 The Customer can configure separate dispositions that are applied to Spam or Probable Spam emails. Those available are: no action; tag the subject; delete the email; quarantine the email.
- 10.4 Approved senders list: Email addresses, domains or IP addresses of email servers can be added to the approved senders list. The content of these entries will not be scanned for Spam and unless they are filtered due to another part of the policy, for example, they contain Malware, they will be delivered.
- 10.5 Blocked senders list: Email addresses, domains or IP addresses of email servers can be added to the blocked senders list and emails addressed from these will be rejected with an appropriate error message.
- 10.6 Approved and blocked senders lists entries can be configured in the KHS using the portal.
- 10.7 Groups functionality allows users or email domains to be grouped together for the purposes of applying policies and for the reporting purposes. Each group can have a different policy applied to it.

### 11 Kaspersky Hosted Email Security. Anti-Malware

- 11.1 The anti-malware functionality of the KHS comprises of several anti-malware technologies to provide maximum security. Anti-malware engines use pattern or signature based technologies as well as heuristic algorithms (Kaspersky BitHunt engine) to protect Customers from zero-hour malware.
- 11.2 Kaspersky BitHunt is a sophisticated and proprietary engine from Kaspersky Lab only available through KHS that protects Customers from zero-hour malware by identifying malicious emails before pattern-based technology.
- 11.3 When Malware is detected in an email an action or disposition is to be taken. This disposition can be configured by the Customer. The options are: add a tag to the Subject field; delete the email; delete an attachment; move the email to quarantine.



## **12 Kaspersky Hosted Email Security. Business Continuity**

- 12.1 Kaspersky Lab continuously monitors the number of emails for each Customer in the queues on its email servers. If a rising email queue is detected for a connected domain, Kaspersky Lab will test for the ability of the receiving mail server to receive email. If Kaspersky Lab is unable to deliver email to a Customer's mail server, Kaspersky Lab will store the Customer's inbound email for up to seven (7) days. During this period Kaspersky Lab will periodically attempt to deliver the queued emails and, when able, will do so in a controlled manner.
- 12.2 Kaspersky Lab offers the Customer access to all inbound emails queued due to the Customer's email server not being able to receive them via a Portal. Those mails are available in the Portal.

## **13 Kaspersky Hosted Email Security. Attachment Handling**

- 13.1 Attachment handling functionality allows control of the size, type and names of attachments to emails.
  - 13.1.1 Kaspersky Hosted Email Security can distinguish between documents, executables, archives, graphics, audio, video and other file types.
  - 13.1.2 A free text field is available to add text (a substring) which can then be compared against the attachment in following ways: name contains substring; name matches substring; extension contains substring; extension matches substring; name or extension contains substring; name or extension matches substring.
- 13.2 Customer can configure how to treat password encrypted files. Available dispositions for the above attachment rules are: no action; tag the subject; delete the email; quarantine the email.

## **14 Kaspersky Hosted Email Security. Quarantine**

- 14.1 All quarantined emails are stored for 30 days and then automatically deleted.
- 14.2 All emails in quarantine can be securely accessed and managed via the Portal.
- 14.3 The quarantine section of the Portal offers text search capability in subject, recipient and sender fields. Following a search, emails meeting the criteria will be displayed with time, sender, recipient, subject, status and size.
- 14.4 From the result page emails can be opened, deleted or released.
- 14.5 Additional and detailed header information is available for each email in quarantine by clicking on the email and the header button.
- 14.6 Blocked and approved senders lists of domain or sender can be modified by clicking the appropriate buttons in the quarantine view.
- 14.7 Users can release quarantined mail via the quarantine report.

## **15 Kaspersky Hosted Email Security. Reports**

- 15.1 Reports can be generated within the Portal. Those available are dependent on the parts of KHS the Customer has licensed.
- 15.2 All reports are available in a graphical (HTML) or PDF format.
- 15.3 Reports can be generated for specified time periods and for specified domains, for mail boxes, groups of mailboxes and groups of domains.
- 15.4 Account summary report shows the number of transactions, categories and volumes.
- 15.5 Reports are available on emails, users, Malware, Spam, phishing and quarantine.
- 15.6 A detailed log can be accessed within the reporting area of the Portal.
- 15.7 Email reports show numbers of emails and the volume of the traffic.
- 15.8 Reports show inbound and outbound traffic.
- 15.9 The quarantine report (QR) provides every user with a report that shows all of their quarantined emails. This report can be requested using the Portal and will be delivered by email or can be run by logging into the Portal.
  - 15.9.1 Reporting Frequency: Daily, weekly, monthly and with a user defined interval.
  - 15.9.2 Reporting Period: today, yesterday, this week, last week, this month, last month.
  - 15.9.3 Information in QR : Reporting period, email count, emails in quarantine and the reason why each was quarantined
- 15.10 Users can initiate the release of quarantined mails while browsing the quarantine report.
- 15.11 Reports are generated in real time.

## **16 Kaspersky Hosted Email Security. Guarantees**



- 16.1 Availability. Kaspersky Lab guarantees an uptime for Kaspersky Hosted Email Security of 99.999%.
- 16.2 In relation to Email Security Availability is defined as the ability to establish an SMTP session on port 25 of the Designated Cluster as measured by Kaspersky Lab. This guarantee shall only apply if all necessary configuration is done by the Customer enabling the Designated Cluster to receive Customer's inbound mail and accept Customer's outbound email on a 24x7 basis.
- 16.3 If in any calendar month Availability is below 99,999%, the Customer may be entitled to the following percentage of credit:

Availability per Calendar Month	Percentage Credit of Monthly Charge
< 99,999% but >= 99,99%	10%
< 99,99% but >= 99%	25%
< 99% but >= 98%	50%
< 98%	100%

- 16.4 In the event Availability falls below ninety eight percent (98%) in any calendar month, the Customer shall be entitled to terminate T&Cs forthwith and receive a refund for that proportion of the fees that relate to the Specified time not used post termination.
- 16.5 In the event that the Customer believes it is entitled to a remedy in accordance with 16.3, the Customer must send a Credit Request within fourteen days (14) of the end of the calendar month in question.
- 16.6 Email Latency. Kaspersky Lab guarantees that the average time to process emails (as measured by Kaspersky Lab by sending Emails every 5 minutes to the Designated Cluster) will be less than 60 seconds. If in any calendar month Latency will exceed the delays stated in the table below, the Customer may be entitled to the following percentage credit:

Average Roundtrip Time per Month	Percentage Credit of Monthly Charge
>1 min but <= 1 min 30 secs	25%
>1 min 30 secs but <= 2 mins	50%
>2 mins but <= 2 min 30 secs	75%
>2 min 30 secs	100%

- 16.7 In the event that the Customer believes it is entitled to a remedy in accordance with 16.6, the Customer must send a Credit Request within fourteen days (14) of the end of the calendar month in question.
- 16.8 Malware Detection: Kaspersky Lab will detect 100% of all Known Malware in the traffic processed by the KHS.
- 16.9 If one or more copies of Known Malware scanned by the KHS are not detected in any calendar month and caused the infection of Customer's systems, Kaspersky Lab will pay any reasonable labour costs directly and demonstrably incurred in removing the Malware from the Customer's network up to a maximum amount equal to 3 Monthly Charges. To receive such cost reimbursement the Customer must send a Credit Request to Kaspersky Lab within 14 days of the occurrence of the breach of this guarantee. The Credit Request shall identify the Malware and the source of infection, demonstrating that the KHS failed to filter out such Malware, and shall enclose proof of costs incurred for which reimbursement is claimed.
- 16.10 The Customer's systems are deemed to be infected if a Virus contained in traffic received through the KHS has been activated within the Customer's systems either automatically or with manual intervention.
- 16.11 The Malware guarantee in clauses 16.8 and 16.9 will not apply if:
- 16.11.1 The Malware was in an email which could not be scanned or analyzed by the KHS (e.g. encrypted or password protected emails);
  - 16.11.2 If Kaspersky Lab notified the Customer immediately following delivery of an email containing the Malware and the Customer failed to take appropriate action;
  - 16.11.3 The Malware was released by the Customer from quarantine;
  - 16.11.4 There was self-infection by the Customer;
- 16.12 Spam Detection Rate: Kaspersky Lab guarantees to detect 98% of all incoming Spam and act in accordance with the policy configured by the Customer using the Portal.
- 16.13 If in any calendar month Spam Detection Rate calculated as the number of correctly identified Spam divided by the sum of the number of correctly identified Spam and the number of False Negatives is below than it is stated in the table, the Customer may be entitled to the following percentage credit:



Spam Detection Rate during the calendar Month	Percentage Credit of Monthly Charge
< 98% but >= 97%	25%
< 97% but >= 96%	50%
< 96% but >= 95%	75%
< 95%	100%

- 16.14 To receive this credit the Customer must send suspected False Negative Emails to [KHS-Support@kaspersky.com](mailto:KHS-Support@kaspersky.com) as an attachment preserving all original e-mail headers within 5 days of receipt of the Email. Kaspersky Lab will investigate and confirm whether or not the Email is a Spam False Negative and will record the finding. At the end of the calendar month if the Customer believes the number of confirmed Spam False Negatives entitles it to a credit in accordance with the clause 16.13, the Customer must send a Credit Request to Kaspersky Lab within 14 days after the end of the respective calendar month.
- 16.15 This guarantee will not apply if:
- 16.15.1 The Customer has not implemented Kaspersky Lab's best practice when configuring the KHS;
- 16.15.2 The email was not sent to a legitimate address.
- 16.16 A lower Spam Capture rate of 95% shall apply to Emails containing Asian and Arabic character sets. In the event that such Spam Capture rate falls below 95% the Customer shall be entitled to a 25% percent credit of the Monthly Charge. In the event that the Spam Capture rate falls below 90% the Customer shall be entitled to a 100% percent credit of the Monthly Charge.
- 16.17 Spam False Positives. Where the average Spam False Positive capture rate rises above 0.0004% of all Customer's email traffic in any calendar month the Customer may be entitled to a credit in accordance with the table below.

Spam False Positives Rate during the calendar Month	Percentage Credit of Monthly Fee
>0.0004% but <= 0.004%	25%
> 0.004% but <= 0.04%	50%
>0.04% but <= 0.4%	75%
>0.4%	100%

- 16.18 To be eligible for a credit in accordance with the clause 16.13, the Customer must send suspected False Positive emails to [KHS-Support@kaspersky.com](mailto:KHS-Support@kaspersky.com) as an attachment within 5 days of receipt of the email. Kaspersky Lab will investigate and confirm whether or not the email is a False Positive and will record the finding. At the end of the calendar month if the Customer believes the number of confirmed False Positives during that calendar month entitles it to a credit in accordance with clause 16.17, the Customer must send a Credit Request to Kaspersky Lab within 14 days after the end of the respective calendar month.
- 16.19 The following emails will not constitute False Positive emails for the purposes of this guarantee:
- 16.19.1 Emails which do not constitute legitimate business email;
- 16.19.2 Where the sender of the email is on the Customer's blocklist;
- 16.19.3 Emails which are sent from a compromised source and rejected according 9.6;
- 16.19.4 Emails which are sent from a machine which is on a third party blocked senders list;
- 16.19.5 Emails which have been sent to more than 20 recipients and have at least 80% the same in content.

## Kaspersky Hosted Web Security

### 17 Overview

- 17.1 The configuration settings required to direct this external traffic via the Kaspersky Hosted Web Security are made and maintained by the Customer and are dependent on the Customer's technical infrastructure. The Customer should ensure that internal HTTP/FTP-over-HTTP traffic (e.g. to the corporate intranet) is not directed via the KHS. Where the Customer has Internet services that mandate a direct connection rather than via a proxy, it is the responsibility of the Customer to make the necessary changes to its own infrastructure to facilitate this.



- 17.2 Once the relevant configuration changes are made requests for Web pages and attachments are electronically routed via the Kaspersky Hosted Web Security and digitally examined for the Malware.
- 17.3 The Customer's external HTTP and FTP-over-HTTP requests including all attachments, macros or executables are directed through the Kaspersky Hosted Web Security. Other content routed through HTTP (for example streaming media) can also be passed through the Kaspersky Hosted Web Security, but shall not be scanned.
- 17.4 Access to the KHS is restricted via Scanning IP i.e. the IP address(es) from which the Customer's web traffic originates. The Scanning IPs are also used to identify the Customer and dynamically select customer-specific settings.
- 17.5 Users can be recognized by IP address of the Customer's gateway or via directory service.
- 17.6 Kaspersky Hosted Web Security will scan as much of the Web page and its attachments as possible. It may not be possible to scan certain Web pages, content or attachments (for example password protected). Attachments specifically identified as unscannable will not be blocked. Streamed and encrypted traffic (i.e. Streaming Media and/or HTTPS/SSL) cannot be scanned and will be passed through Kaspersky Hosted Web Security unscanned.
- 17.7 Kaspersky Lab emphasizes that the configuration of Kaspersky Hosted Web Security is entirely under the control of the Customer. The KHS described in this KHS Description is intended to be used solely to enable the Customer to enforce an existing, effectively implemented Acceptable Computer Use Policy (or its equivalent). In certain countries it may be necessary to obtain the consent of individual personnel and so Kaspersky Lab advises the Customer to always check their local legislation prior to deploying Kaspersky Hosted Web Security.
- 17.8 User emails can be defined by the administrator to inform user if a virus or spyware was detected.
- 17.9 The administrator can create a white list for adware programs.

## **18 Kaspersky Hosted Web Security. Reporting**

- 18.1 Summary reports can be drawn on a daily, weekly, monthly or yearly basis.
- 18.2 Summary reports can be generated as graph, xml, csv or table.
- 18.3 Scheduled report can be generated based on:
  - 18.3.1 Top Viruses blocked
  - 18.3.2 Blocked Viruses by number of hits
  - 18.3.3 Top Groups by blocked viruses
  - 18.3.4 Protocol trend by bandwidth
  - 18.3.5 Protocol trend by connections
  - 18.3.6 Top users by blocked viruses
  - 18.3.7 Allowed Traffic Reports
  - 18.3.8 Blocked Traffic Reports
- 18.4 Frequency for scheduled reports can be
  - 18.4.1 Once only
  - 18.4.2 Daily
  - 18.4.3 Weekly
  - 18.4.4 Monthly
- 18.5 Forensic Reports can be generated for specific users or groups on a custom period.

## **19 Kaspersky Hosted Web Security. Virus Scanning (AV)**

- 19.1 Once the relevant configuration changes are made Web pages and attachments will be scanned by industry leading anti-virus engines.
- 19.2 AV will scan as much of the Web page and its attachments as possible. It may not be possible to scan certain Web pages or attachments (for example, password protected). Unscannable attachments will be blocked. Encrypted traffic (i.e. HTTPS/SSL) cannot be scanned and will be passed through AV unscanned.
- 19.3 If a Customer's Web page or attachments are found to contain a Malware (or deemed unscannable), then access to that Web page or attachment is denied and the Internet user will be displayed an automatic virus alert Web page. Notification may also be sent by email to a Customer administrator.
- 19.4 AV will scan the first 100Mb of each file transfer. Where files are downloaded that exceed 100Mb in size, the initial 100Mb will be scanned and the remainder passed through.

## **20 Kaspersky Hosted Web Security. Spyware Screening (SPS)**



- 20.1 Once the relevant configuration changes are made Web pages and attachments will be scanned and filtered.
- 20.2 SPS will scan as much of the Web pages or attachments as possible. It may not be possible to scan certain Web pages or attachments (for example, password protected). Unscannable attachments will be blocked. Encrypted traffic (i.e. HTTPS/SSL) cannot be scanned and will be passed through SPS unscanned.
- 20.3 If a Customer's Web page or attachments are found to contain Spyware (or deemed unscannable), then access to that Web page or attachment is denied and the Internet user will be displayed an automatic spyware alert Web page. Notification may also be sent by email to a Customer administrator.
- 20.4 SPS will scan the first 100Mb of each file transfer. Where files are downloaded that exceed 100Mb in size, the initial 100Mb will be scanned and the remainder passed through.

## **21 Kaspersky Hosted Web Security. Web Filtering (WF)**

- 21.1 Once the relevant configuration changes are made Web pages and attachments will be filtered using URL categorization and content analysis. URLs are categorized by reference to a number of predefined categories as specified in Portal.
- 21.2 The Customer is able to configure Web Filtering to create access restriction policies (based both on categories and types of content) and deploy these at specific times to specific Internet users or groups. A number of additional features (for example, approved and blocked URLs list functionality) are also available.
- 21.3 WF will filter as much of the Web page and its attachments as possible. It may not be possible to filter certain Web pages or attachments (for example, password protected). Customers may also configure specific exceptions for web sites that should not be filtered. Encrypted traffic (i.e. HTTPS/SSL) cannot be filtered and will be passed through WF unless otherwise specified by the Customer in relation to specific categories of content. WF will only filter Web pages that are categorized by WF in accordance with the category that the Customer has chosen to filter.
- 21.4 The Customer has the option of performing individual and/or group administration and reporting capabilities by utilizing the relevant Agent software application. Use of the Agent application will be subject to the End User License Agreement provided with the application.
- 21.5 If an Internet user requests a Web page or attachment where an access restriction policy applies, then access to that Web page or attachment is denied and the user will be displayed an automatic alert Web page. Notification may also be sent by email to a Customer administrator.

## **22 Kaspersky Hosted Web Security Connector**

- 22.1 Kaspersky Lab will make available optional software ("Connector") to Customers. If ordered by the Customer, Kaspersky Lab will provide the Connector software to the Customer to install in their network in accordance with Kaspersky Lab's installation guidelines. There are two types of Connector:
  - The Workgroup Connector is for Customers with a simple network configuration. It enables the identification of individual users when they access the Services (using a license key). Customers are therefore able to use the Portal to apply policies, administer and report against individual users or groups as defined within existing Customer directories and as supported by the Connector. The Workgroup Connector will run in standalone mode and provides both forwarding and AD integration.
  - The Enterprise Connector is for Customers who already have edge devices (e.g. ISA Server, Checkpoint, Cisco, Blue Coat) and need to integrate the KHS with them.
- 22.2 The Connector enables users to connect to the Services even without a static IP address by using a license key. If users have other services that rely on a fixed IP address for identification, they can configure direct connections for specific websites, domains, hosts or networks.
- 22.3 Administrators can create, revoke, activate, and deactivate license keys for connectors per group or per users.
- 22.4 The Connector does not support all potential Customer systems and set-ups. For the technical information see <http://support.kaspersky.com/faq/?qid=208281752>.

## **23 Kaspersky Hosted Web Security. Guarantees**

- 23.1 Availability. Kaspersky Lab guarantees an uptime for Kaspersky Hosted Web Security of 99.999%.
- 23.2 Uptime for Kaspersky Hosted Web Security is defined as the ability to accept the Customer's outbound web requests and shall only apply if the Customer host, gateway devices or proxy(s) are correctly configured on 24x7 basis.
- 23.3 All measures of the described functionalities and guarantees are defined for a given calendar month.
- 23.4 In the event that Kaspersky Lab fails to meet Availability commitment set out in the table below, the Customer may be entitled to the following percentage credit:



Availability per Calendar Month	Percentage Credit of Monthly Charge
< 99,999% but >= 99,99%	10%
< 99,99% but >= 99%	25%
< 99% but >= 98%	50%
< 98%	100%

23.5 To receive the credit the Customer must send a Credit Request to [KHS-Support@kaspersky.com](mailto:KHS-Support@kaspersky.com) within 14 days of the occurrence of the breach of this guarantee.

