TERMS AND CONDITIONS

KASPERSKY MANAGED PROTECTION SERVICE

WHEREAS, the Customer named in the corresponding order ("Customer") desires to acquire the Kaspersky Managed Protection Service ("KMP" or "Service") of Kaspersky Lab ("Kaspersky Lab" or "Kaspersky") and Kaspersky Lab desires to render Service to the Customer;

NOW THEREFORE, in consideration of the mutual covenants and promises in these Terms and Conditions ("T&C") and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, and by Customer purchasing the Service in accordance with the related ordering process and/or clicking the appropriate buttons if required by Kaspersky Lab to confirm and accept this T&C (which to the maximum extent permitted under applicable law shall be deemed conclusive approval thereof), the parties agree as follows:

Kaspersky Lab agrees to render Service in the manner and within the time period in accordance with the Order for the Service placed within Kaspersky Lab Ordering System ("Order"), this T&C and applicable agreement that can be whether direct agreement between Kaspersky Lab and Customer, or agreement concluded by the Customer with corresponding authorized partner of Kaspersky Lab ("Partner").

1. SERVICE DESCRIPTION

Service Goal and Objectives
The main goal of the Service is to give the Customer early information about threats by proactively receiving data provided by the Customer to Kaspersky Lab meta-data of network and system activity. It allows detection of both known and unknown threats.

Investigation is conducted by Kaspersky Lab analysts to recognize that event or complex of events being monitored on the Customer's side as a true incident and to avoid false positives only.

Incident is a critical event or complex of events discovered during execution of the Service.

Kaspersky Lab provides incident management in accordance with Section 2 of this T&C.

Monitoring Options
- Advanced Kaspersky Endpoint Security ("KES") monitoring;
- Kaspersky Anti Targeted Attack Platform ("KATA") and advanced KES monitoring.

Within the service, the following tasks should be solved:
- Monitoring of events generated by KES implemented in Customer's network;
- Monitoring of events generated by KATA implemented in Customer's network;
- Analysis of obtained information with Kaspersky Security Network ("KSN") technology;
Analysis of gathered information for traces presence of targeted attacks;
Timely informing the Customer when a threat is detected and actions from the Customer are needed;
Provide recommendations for response to detected threats.

Kaspersky Lab provides Customer the Service option indicated in the Order in accordance with this T&C.

Service Options:
- System to be monitored according to the installed software within the Customer infrastructure: KES; KATA or KATA+KES;
- According to the maintenance mode below: 24/7 or 5/8;
- According to the Number of Endpoints within the Customer infrastructure to be monitored.

Incident Management

Incident default level of priority is “Low”.

Kaspersky Lab provides management of incidents according to the maintenance modes by working support groups of analysts set forth in this section of the T&C.

Maintenance Modes

<table>
<thead>
<tr>
<th>Maintenance Mode</th>
<th>Description</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>8x5 (GMT+3)</td>
<td>Monday-Friday: 10:00 – 18:30</td>
<td>All automatic systems continue to work 24x7 and all incidents are detected. Working groups operate in 8x5 modes, so analysis of data is performed 8x5. All events collected by sensors, irrespective of whether they occurred 24x7 or 8x5 is analyzed. Operation mode influence only on SLA calculation and not affect data to be analyzed.</td>
</tr>
<tr>
<td>24x7</td>
<td>Around-the-clock, including weekends and holidays</td>
<td>All automatic systems and working groups operate in 24x7 mode.</td>
</tr>
</tbody>
</table>

Support Groups of Analysts

<table>
<thead>
<tr>
<th>Line Support</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st Tier</td>
<td>Monitoring Service Analyst</td>
</tr>
<tr>
<td>2nd Tier</td>
<td>Malware Analyst</td>
</tr>
</tbody>
</table>
Scenario 1: Incident Detection by 1st Tier support

In Scenario 1, Monitoring Service Analyst discovered the incident. Incidents discovered by detection systems are recorded in incident tracking system automatically. Manually detected incidents are registered in incident tracking system by Monitoring Service Analyst. Priority default level of incident can be changed later but with necessarily note of change reason according to the Incident Priority Level set forth in the T&C.

Monitoring Service Analyst processes recorded events to promptly obtain information about Customer’s IT infrastructure.

If analysis showed causes of incident, Customer will be provided with the response recommendations. Otherwise, all gathered information and analysis results are transferred to the Customer to arrange further investigation on the Customer’s side.

Scenario 2: Incident Detection by Customer

In Scenario 2, Customer sends all available information about discovered incident by encrypted email communication to the email address: SOC@kaspersky.com. PGP key from the Customer is required. Monitoring Service Analyst requests missing information if necessary.

Incident priority level is set to default, unless otherwise specified by the Customer.

The rest of procedure is similar to Scenario 1.

Incident Priority Levels

<table>
<thead>
<tr>
<th>Priority level</th>
<th>Incident details</th>
<th>Reporting procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Traces of targeted attack or unknown threat, requires further investigation using digital forensic methods</td>
<td>Operatively by email</td>
</tr>
<tr>
<td>Normal</td>
<td>Malware – Trojan, Cryptor and etc.</td>
<td>Weekly</td>
</tr>
<tr>
<td>Low</td>
<td>Potential unwanted software – Adware, Riskware, not-a-virus and etc.</td>
<td>Weekly</td>
</tr>
</tbody>
</table>

Target values of the Service delivery

<table>
<thead>
<tr>
<th>Priority level</th>
<th>Reaction time</th>
<th>Target value</th>
<th>Response time</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>4 hours</td>
<td>90%</td>
<td>unknown</td>
</tr>
<tr>
<td>Medium</td>
<td>16 hours</td>
<td></td>
<td>16 hours</td>
</tr>
<tr>
<td>Low</td>
<td>24 hours</td>
<td></td>
<td>24 hours</td>
</tr>
</tbody>
</table>

1- Reaction time – the time from detection of incident (status “New”) prior to taking it into work by Monitoring Service Analyst (status “1st line support”).

2- Target Value – percent of the number of incidents with Reaction time and Response time met Target value objective.

3- Response time – the time from taking to work by monitoring service analyst (status “1st line support”) until incident is solved (status “Resolved”).
Incident is solved if the Customer has been provided with recommendations for response measures. The Service does not include any incident response activities.

Kaspersky Lab reserves the right to store the collected information in accordance with this T&C and its Appendixes, unless otherwise is not specified by the Customer.

### Incident Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The following values are possible:</td>
</tr>
<tr>
<td></td>
<td>• “New” - Registered incident, but not taken into work;</td>
</tr>
<tr>
<td></td>
<td>• “1st Tier investigation” - Incident taken into work by Monitoring Service Analyst;</td>
</tr>
<tr>
<td></td>
<td>• “2nd Tier investigation” - Incident taken into work by malware analyst;</td>
</tr>
<tr>
<td></td>
<td>• “Resolved” - Incident solved by Kaspersky Lab, but still some actions required from Customer;</td>
</tr>
<tr>
<td></td>
<td>• “On hold” - Work on the incident shall be suspended whenever the expected decision or completion of work by Customer;</td>
</tr>
<tr>
<td></td>
<td>• “Pending close” - Incident put in this status, when all the work on the incident, including the work on the part of the Customer have been completed;</td>
</tr>
<tr>
<td></td>
<td>• “Closed” - Incident with status &quot;Pending close&quot; switches automatically within 3 working days to status &quot;Closed&quot;.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status description</th>
<th>Kaspersky Lab comments to the status.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolution</td>
<td>It characterizes the quality of incident detection. The field is adjusted based on the results of the investigation of the incident. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• True positive</td>
</tr>
<tr>
<td></td>
<td>• False positive</td>
</tr>
</tbody>
</table>

The following types of False positives are taking into account:

“Infr” – infrastructure false positive means that detection technology worked properly, but taking into account the Customer’s context for this particular event infrastructure is not an incident; analysis of this types of false positives allows to adapt the monitoring service to the context of the customer’s infrastructure; example is the detection of access to a malicious site that is blocked by content filtering system.
“Tech” – technological false positive - incorrect work of the detection logic (signature); analysis of this type allows to improve the detection mechanisms; example is incorrect detect of innocent file as malicious.

<table>
<thead>
<tr>
<th>FP reason</th>
<th>Type of false positive (Infr, Tech)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack stage</td>
<td>Stage in Attack Kill Chain. The following stages are possible:</td>
</tr>
<tr>
<td></td>
<td>• Recon – initial reconnaissance;</td>
</tr>
<tr>
<td></td>
<td>• Initial compromise;</td>
</tr>
<tr>
<td></td>
<td>• Persistence establishment;</td>
</tr>
<tr>
<td></td>
<td>• Privileges escalation;</td>
</tr>
<tr>
<td></td>
<td>• Internal recon;</td>
</tr>
<tr>
<td></td>
<td>• Post-exploitation.</td>
</tr>
</tbody>
</table>

**Reports**

Reports are provided in accordance with the below timeframes in English language.

<table>
<thead>
<tr>
<th>Report name</th>
<th>Timeframes</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of all incidents processed during the</td>
<td>Weekly for the previous week</td>
</tr>
<tr>
<td>reporting period</td>
<td>Monthly for the previous month</td>
</tr>
<tr>
<td>Incident card</td>
<td>Promptly available for incidents with “High”</td>
</tr>
<tr>
<td></td>
<td>priority level after taking into work.</td>
</tr>
<tr>
<td></td>
<td>Available on Customer request for incidents</td>
</tr>
<tr>
<td></td>
<td>with “Medium” or “Low” priority level.</td>
</tr>
</tbody>
</table>

Weekly reports provided no later than 12:00 (GMT+4) each Monday.

Monthly reports provided no later than 12:00 (GMT+4) of the 5th of each month.

**2. SERVICE DELIVERY**

2.1. **Service Activation.**

- KSN activation of Kaspersky Endpoint Security and/or Kaspersky Anti Targeted Attack Platform (depending on monitoring options) is mandatory for the enabling provision of Service in due order. Customer understands and accepts that if receiving data through KSN is not activated Kaspersky Lab will not be able to provide the Service.

- Service rendering for KES starts after provision of the license serial number by the Customer to Kaspersky Lab. After license serial number is provided Kaspersky Lab experts send to the Customer a report containing a list of the Customer endpoints protected by KES. Customer have to confirm the list is complete. In case of missing endpoints in the list Kaspersky Lab experts take up to ten (10) business days to investigate the case and include missing endpoints to the monitored list.
• Service execution for KATA starts after provision of the installation ID by the Customer to Kaspersky Lab. After installation ID is provided Kaspersky Lab experts confirm availability of KATA notifications for analysis. In case of no notifications corresponding specified installation ID were found Kaspersky Lab experts take up to ten (10) business days to investigate the case and provide the solution.

• Kaspersky Lab starts the Service provision within thirty (30) days after the Order for the Service is placed within Kaspersky Lab Ordering.

All the necessary information should be provided by the Customer to the following email address: SOC@kaspersky.com.

2.2 Conditions. The Service is provided remotely. The Customer accepts and authorizes that Kaspersky Lab automatically receives information needed for providing qualitative Service to the Customer. Information being collected during execution of the Service set forth at the Appendixes to the T&C:

• Appendix 1 lists the information being automatically received during KES advanced monitoring;
• Appendix 2 lists the information being automatically received during KATA monitoring.

2.3 Term. This T&C shall commence on the effective date, which is the date of acceptance of this T&C by Customer. The T&C shall terminate as soon as period of the Service provision is expired unless the initial term of the Service is extended or renewed by a new Order.

2.4 Compensation. The Service fee and payment details and order shall be stipulated in the Order or in the applicable agreement. Obligations of Kaspersky Lab hereunder shall be subject to and conditioned upon the confirmation from Customer that the payment terms for the Service have been fully accepted and acknowledged by Customer and Kaspersky Lab received a valid Order in respect of this Service. Customer hereby agrees to pay fees for Service in due order including all applicable taxes.

2.5 Service Limitation. Service not specifically set forth in this T&C is considered out of the Service scope. The following services are explicitly excluded from the Service: Incident Response, Malware Analysis and Digital Forensic. Other services that may be recommended by Kaspersky Lab during the Service provision may be purchased by Customer additionally via another Order.

2.6 Cooperation. Customer shall provide the access to its information and property as may be reasonably required in order to permit Kaspersky Lab to perform its obligations hereunder. Kaspersky Lab will not be liable if information or materials provided to Kaspersky Lab by the Customer are unavailable, inaccurate, and/or inadequate for providing the Service. Kaspersky Lab will use commercially reasonable efforts to work with the Customer to correct or clarify any inaccuracies in the Customer’s information or materials.

2.7 Warranties. Kaspersky Lab warrants that the Service will be provided by experienced, qualified personnel on a reasonable efforts basis consistent with reasonable industry standards in a professional and workmanlike manner, and further warrants that Kaspersky Lab has the required skills and experience to render the Services. EXCEPT AS EXPlictLY SET FORTH HEREl, THE SERVICE IS PROVIDED TO THE CUSTOMER "AS IS"
AND WITHOUT WARRANTY OF ANY KIND. KASPERSKY LAB DOES NOT MAKE ANY OTHER
REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE
SERVICE, THE RESULTS TO BE OBTAINED THEREFROM, OR AS TO THE MERCHANTABILITY
OR FITNESS FOR A PARTICULAR PURPOSE. NEITHER PARTY WILL HAVE ANY LIABILITY IN
TORT, CONTRACT OR OTHERWISE, FOR ANY INDIRECT, SPECIAL, INCIDENTAL,
CONSEQUENTIAL (INCLUDING LOST PROFITS), OR PUNITIVE DAMAGES, ARISING OUT OF
THIS T&C, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND IN NO CASE
WILL THE LIABILITY OF EITHER PARTY EXCEED THE TOTAL CHARGES PAID BY THE
CUSTOMER FOR THE SERVICE PROVIDED UNDER THIS T&C.

2.8. Confidentiality. With respect to Customer Data provided by the Customer to
Kaspersky Lab hereunder that is identified by the Customer as being confidential, Kaspersky
Lab agrees to take such security measures to prevent the unauthorized duplication,
distribution, disclosure or use of the Customer Data equal to that which Kaspersky Lab uses
to protect its own proprietary information, and in no event these measures will be less than
commercially reasonable.

2.9. Any pre-existing proprietary or Confidential Information of Kaspersky Lab used to
render the Services, or included into the results or deliverables of the Service provision,
including but not limited to software, appliances, methodologies, code, templates, tools,
policies, records, working papers, know-how, data or other intellectual property, written or
otherwise, shall remain Kaspersky Lab exclusive property.

3. SERVICE USE

3.1. Customer may use the Service only upon of execution of this T&C.

3.2. Customer may not distribute, transfer or resell information delivered during the
Service provision (including content, format, delivery, update details, number of records,
sources of intelligence and internal manuals). Customer may use the Service and any results
of Services including without limitation deliverables, materials documentation related to the
Services only for internal use purposes to protect its own infrastructure and its own
employees. Providing of any above indicated results of Services to the third parties
regardless of whether they are provided on commercial or free basis is strictly prohibited
and considered as significant harm to Kaspersky Lab. In case if Customer violates
restriction indicated hereof Kaspersky Lab shall be entitled to charge compensation which may include
direct damages as well as loss of profit and any supplementary expenses which may be
suffered by Kaspersky Lab subject to this violation and Customer hereby agrees that
payment of such compensation shall not be unreasonably withheld.

3.3. Customer acknowledges that Kaspersky Lab provides various services same or
similar to the Service to other customers and that nothing in the T&C shall be construed to
prevent Kaspersky Lab from carrying on such business. Customer acknowledges that
Kaspersky Lab may at its sole discretion develop, use, market, distribute any deliverables
that is substantially similar to deliverables of the Service with similar structure, content and
organization. Notwithstanding the preceding sentence, Kaspersky Lab agrees that it will not
market or distribute any deliverables that include confidential information of Customer.

3.4. Customer agrees that the Service and the authorship, systems, ideas, methods of
operation, documentation and other information contained in the Service or related to
rendering of Services, are proprietary intellectual property and/or the valuable trade secrets
of Kaspersky Lab and that Kaspersky Lab, as applicable, is 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. This T&C does not grant to the Customer any rights to the intellectual property including any trademarks or service marks of Kaspersky Lab (“Trademarks”). Customer may use the Trademarks only insofar as to identify printed output produced by the Service in accordance with accepted trademark practice, including identification of the Trademark owner’s name. Such use of any Trademark does not give to the Customer any rights of ownership in that Trademark. Kaspersky Lab owns and retains all right, title, and interest in and to the Service, including without limitation any error corrections, enhancements, Updates or other modifications to the Service, whether made by Kaspersky Lab or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. Customer’s use of the Service does not transfer to the Customer any title to the intellectual property in the Service. Except as stated herein, this T&C does not grant the Customer any intellectual property rights included into the results or deliverables of the Service. Kaspersky Lab reserves all rights not expressly granted to the Customer in this T&C.

3.5. Violation of the intellectual rights to the Service shall result in civil, administrative or criminal liability in accordance with the law.

3.6. Customer may not remove or alter any copyright notices or other proprietary notices on any copies of the Service or its results.

3.7. Customer has the right to keep Service deliverables related documentation and materials.

3.8. Kaspersky Lab reserves the right to improve the Service by changing its components (including without limitation content, format, delivery, update details, number of records, sources of intelligence and internal manuals).

3.9. EXCEPT FOR KASPERSKY LAB OBLIGATIONS STATED HEREBY THE SERVICE IS PROVIDED “AS IS” AND KASPERSKY LAB MAKES NO REPRESENTATION AND GIVES NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW KASPERSKY LAB MAKES NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESSED OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR APPLICABILITY FOR A PARTICULAR PURPOSE. CUSTOMER ASSUMES ALL FAULTS, AND THE ENTIRE RISK AS TO PERFORMANCE AND RESPONSIBILITY FOR SELECTING THE SERVICE, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SERVICE. WITHOUT LIMITING THE FOREGOING PROVISIONS, KASPERSKY LAB MAKES NO REPRESENTATION AND GIVES NO WARRANTY THAT THE SERVICE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SERVICE WILL MEET ANY OR ALL YOUR REQUIREMENTS WHETHER OR NOT DISCLOSED TO KASPERSKY LAB.

3.10. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL KASPERSKY LAB BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO,
DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR LOSS OF PRIVACY, FOR CORRUPTION, DAMAGE AND LOSS OF DATA OR PROGRAMS, FOR FAILURE TO MEET ANY DUTY INCLUDING ANY STATUTORY DUTY, DUTY OF GOOD FAITH OR DUTY OF REASONABLE CARE, FOR NEGLIGENCE, FOR ECONOMIC LOSS, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SERVICE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SERVICE AND RELATED CONTENT THROUGH THE SERVICE OR OTHERWISE ARISING OUT OF THE USE OF THE SERVICE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS T&C, OR ARISING OUT OF ANY BREACH OF CONTRACT OR ANY TORT (INCLUDING NEGLIGENCE, MISREPRESENTATION, ANY STRICT LIABILITY OBLIGATION OR DUTY), OR ANY BREACH OF STATUTORY DUTY, OR ANY BREACH OF WARRANTY OF KASPERSKY LAB, EVEN IF KASPERSKY LAB HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

3.11. If Customer violates any of its obligations hereof or Service limitations stipulated in this T&C or other legally binding document concluded between Kaspersky Lab and Customer, Kaspersky Lab may stop rendering of Service or deliver the Service with limited scope.

3.12. Customer agrees to be responsible for legal compliance of using Service within the Customer infrastructure and industry.

3.13. Kaspersky Lab reserves the right at any time to modify this T&C and to impose new or additional terms or conditions on the Service use. Such modifications will be effective immediately when incorporated into the T&C. Continued use of the Service by Customer will be deemed acceptance thereof.

3.14. No delay or omission by either party in exercising any right under this T&C shall operate as a waiver of that or any other right. A waiver or consent given by a party on any one occasion shall be effective only in that instance and shall not be construed as a bar or waiver of any right on any other occasion. In the event that any provision of this T&C shall be invalid, illegal or otherwise unenforceable, the validity, legality and enforceability of the remaining provisions shall in no way be affected or impaired. This T&C may also be amended or modified by a written instrument executed by both the Customer and Kaspersky Lab or by Kaspersky Lab only as stipulated in clause 3.13.

3.15. All disputes arising out of or in connection with this T&C, including any question regarding its existence, validity or termination, shall be referred to and finally settled under the Rules of Arbitration of the International Chamber of Commerce, which Rules are deemed to be incorporated by reference into this section. The number of arbitrators shall be three. The seat of arbitration shall be London, England. The procedural law of this place shall apply where the Rules are silent. The language to be used in the arbitration proceeding shall be English. The governing law of the Agreement shall be the substantive law of England and Wales.

This T&C shall be binding upon, and inure to the benefit of, both parties and their respective successors and assigns.
APPENDIX 1

List of information provided during Kaspersky Endpoint Security Advanced monitoring.

In order to identify new and challenging data security threats and their sources, as well as threats of intrusion, and to take prompt measures to increase the protection of the data stored and processed by the Customer with a computer, the Customer agrees to automatically provide the following information in order to get the Service:

- Date of software installation and activation, the full software version, including information about installed updates and the software's locale;
- Information about the software installed on the computer, including the version of the operating system and installed updates, kernel objects, drivers, services, Microsoft Internet Explorer extensions, printing system extension, Windows Explorer extensions, downloaded objects checksums (MD5), Active Setup elements, control panel applets, versions of browsers and mail clients;
- Information about the computer's name, IP-addresses and hardware, including a checksum of the HDD's serial number;
- Data about software tools used to fix problems in software installed on the Customer's computer, or to change its functionality, and the return codes received after the installation of each piece of software;
- Information about the state of the computer's anti-virus protection, including the versions and release dates and times of the anti-virus databases being used, statistics about updates and connections with Kaspersky Lab services, job identifier and the identifier of the software component performing scanning;
- Information about files (file name, size, MD5-hash, file content is not provided) being downloaded by the Customer, including the URL and IP addresses of the download and the download pages (content of pages is not provided, only URL), download protocol identifier and connection port number, the status of the URLs as malicious or not, file’s attributes, size and checksums (MD5, SHA2-256, SHA1), information about the process that downloaded the file (checksums (MD5, SHA2-256, SHA1), creation/build date and time, autoplay status, attributes, names of packers, information about signatures, executable file flag, format identifier, and entropy), file name and its path, the file’s digital signature and timestamp of its generation, the URL where detection occurred, the script's number on the page that appears to be suspicious or harmful, information about HTTP requests generated and the response to them;
- Information about the running applications and their modules, including information about processes running on the system (process ID (PID), process name, the application and command that started the process, the full path to the process’s files, and the starting command line, a description of the product that the process belongs to (including the name of the product and information about the publisher), as well as digital certificates being used and information needed to verify their authenticity or information about the absence of a file’s digital signature), and information about the modules loaded into the processes, including their names, sizes, types, creation
dates, attributes, checksums (MD5, SHA2-256, SHA1), the paths to them, PE-file header information, names of packers (if the file was packed);

- Information about all potentially malicious objects and actions, including the name of the detected object and the full path to the object on the computer, checksums (MD5, SHA2-256, SHA1) of the files being processed, detection date and time, names and size of downloaded files and paths to them, code of the path template, names of packers (if the file was packed), file type code, file format identifier, list of the activities of malicious applications and associated decisions made by the software and the Customer, identifiers for the anti-virus databases the software used to make a decision, name of the detected threat according to Kaspersky Lab's classification, danger level and detection status, reason for including a file in the analyzed context and the file's serial number in the context, checksums (MD5, SHA2-256, SHA1), name and attributes of the executable file for the application that passed the infected message, anonymized IP address (IPv4 and IPv6) of the blocked object's host, the file's entropy, autoplay status, time of the file's first detection in the system, number of times the file has been run since the last time statistics were sent, information about the name, checksums (MD5, SHA 256, SHA1) and size of the mail client used to receive the malicious object, identifier of the entry in the anti-virus databases used to arrive at a verdict, job identifier of the software that performed the scan, flag of the reputation verification or file signature verification, result of processing the file, checksum (MD5) of the pattern collected on the object and pattern size in bytes;

- Information about scanned objects, including the assigned trust group to which and/or from which the file has been placed, the reason the file was placed in that category, category identifier, information about the source of the categories and the version of the category database, the file’s trusted certificate flag, name of the file’s vendor, file version, name and version of the software product which includes the file;

- Information about vulnerabilities detected, including the vulnerability ID in the database of vulnerabilities, the vulnerability danger class, and the status of detection;

- Information about emulation of the executable file, including file size and its checksums (MD5, SHA2-256, SHA1), the version of the emulation component, emulation depth, an array of properties of logical blocks and functions within logical blocks obtained during the emulation, data from the executable file’s PE headers;

- Information about network attacks, including the IP addresses of the attacking computer (IPv4 and IPv6), the number of the port on the Customer’s computer that the network attack is directed at, identifier of the protocol of the IP packet containing the attack, flag for the reaction to the attack, the attack’s weight, trust level;

- Information about attacks associated with spoofed network resources, including the DNS and IP addresses (IPv4 and IPv6) of visited websites, number of IP address assignments for the domain name;

- Information about the rolling back of malware’s activities, including data about the file whose activities are being rolled back (file name, full path to the file, its size and checksums (MD5, SHA2-256, SHA1)), data about successful and unsuccessful actions to delete, rename, and copy files and restore values in the registry (names of registry keys and their values), information about system files changed by malware, before and after the roll back;
Information about the loaded software modules, including name, size and checksums (MD5, SHA2-256, SHA1) of the module file, its full path and template code of the file path, parameters of the module file’s digital signature, timestamp of the signature generation, names of the subject and the organization that signed the module file, identifier of the process, in which the module was loaded, name of the module vendor, index number of the module in the load queue;

Information to determine the reputation of files and URL-addresses, including checksums of the scanned file (MD5, SHA2-256, SHA1) and pattern (MD5) obtained during the emulation of the file, size of the pattern, emulation depth, the version of the emulation component, type of the detected threat and its name according to Kaspersky Lab’s classification, identifier for the anti-virus databases, URL address at which the reputation is being requested, as well as the referrer URL address, the connection’s protocol identifier and the number of the port being used;

Service information about the software’s operation, including the compiler version, flag for the potential maliciousness of the scanned object, version of the set of statistics being sent, information about the availability and validity of these statistics, identifier of the mode for generating the statistics being sent, flag indicating whether the software is operating in interactive mode;

Information about events in the systems logs, including the event’s timestamp, the name of the log in which the event was found, type and category of the event, name of the event’s source and the event’s description;

Information about network connections, including version and checksums (MD5, SHA2-256, SHA1) of the file from which process was started that opened the port, the path to the process's file and its digital signature, local and remote IP-addresses, numbers of local and remote connection ports, connection state, timestamp of the port’s opening.

For incident investigation within the Service the Customer agrees to provide upon request files or parts of files.

In order to receive the reference information about the number of objects with known reputation, the Customer agrees to provide information about the version of the protocol used to connect with the Rightholder’s services.

When participating in Kaspersky Security Network (“KSN”), the Customer agrees to provide the following information for all purposes mentioned above:

- The unique software installation identifier;
- The full version of the installed software;
- The type identifier of the installed software;
- The unique identifier of the computer with the installed software.
APPENDIX 2.

List of information provided during Kaspersky Anti-Targeted Attack Monitoring.

In order to identify new and challenging data security events and their sources, as well as threats of intrusion, and to take prompt measures to increase the protection of the data stored and processed by the Customer with a computer, the Customer agrees to automatically provide the following information in order to get the Service:

- Information about the identifier, version, type, and timestamp of the record in the anti-virus database used to detect an information security event, the name of the threat based on the Right Holder's classification, timestamp of the anti-virus databases being used, file type code, file format identifier, the task identifier of the software that detected the event, flag of the reputation verification or file signature verification;

- Information to determine the reputation of files and web-resources, including IP-address and the domain name of the URL-address at which the reputation is being requested, as well as checksum (MD5) of the domain name, the name of the file, that was executed when an event is detected, the path to the file, and checksums (MD5) of the file and its path;

- Information about emulation of the executable file, including file size and its checksums (MD5, SHA2-256, SHA1), the version of the emulation component, emulation depth, an array of properties of logical blocks and functions within logical blocks obtained during the emulation, data from the executable file’s PE headers;

- Information about all detected objects, including the name and size of the object, the full path to the object on the computer, checksums (MD5, SHA2-256) of the files being processed, the name of the event associated with the object, detection date and time, flag of the presence of the file's digital signature, the name of the organization that signed the file, the trust status and threat level of the file, the identifier and priority of the rule used for detection, and the type of detection technology;

- The type of source from which the object was downloaded, the source’s IP-address (or checksum (MD5) of the IP-address, when it is local), the source’s URL-address, as well as the referrer URL address, the name, the domain’s name and checksum (MD5) of the name of the host, that sent the downloading request, the service information about the web-browser, that sent the downloading request;

- Checksums (MD5) of the local and domain parts of the sender’s and the receiver’s email addresses, as well as checksum (MD5) of the email’s subject;

- The local and remote IP-addresses of the network connection (or checksum (MD5) of the IP-address, when it is local), the numbers of the local and remote ports and the connection’s protocol identifier;

- The URL-address and the name of the target host, and the host's IP-addresses (or checksum (MD5) of the IP-address, when it is local);

- The identifier of the operating system, that is installed on a virtual machine, which is used by the software to analyze objects;
Additional information about events, including the frequency index of the file in the Customer’s local network, the date of the file’s intrusion in the local network and on the Customer’s computer, the identifiers of the accounts the process was started from, checksums of their user names, as well as the names of their domains or workgroups, information about the privileges of the user accounts;

Information about the network activity of the process, including the domain names of the network resources that used to establish a connection, and IP-addresses of the domains (or checksum (MD5) of the IP-address, when it is local), the frequency of the connection with the selected network resource, the size and type of the transferred data;

Information about the network activity of the process in the local network, including the port numbers, the socket addresses and checksums (MD5) of the IP-addresses, to which the process sent requests;

The file names of the processes with which the process interacted, the filenames of the modules that were loaded by the process, the names of registry keys and their values that were modified by the process, and the normalized paths to the files and registry keys;

The names of the synchronization objects that were modified by the process;

Information about the usage of the domain of the network resource, including the frequency index of the requests to the domain from the local network, the timestamp of the first request to the domain from the local network, the duration of the requests from different users and checksums of the their names, the names of the computers that initiated the requests to the domain, and checksums (MD5) of the IP-addresses of these computers, additional information about detection reasons;

Service information about the statistics processing component, including the date and time of the beginning and the end of the term that was used to analyze the statistics data, the volume of the free and used disk memory, the time of the last event processing, the operating time of different detection algorithms, messages about the component’s errors, messages about the successful start of different detection algorithms;

The version of the operating version installed on the computer, the version of the set of statistics being sent, the notification creation time, the type of client application that initiated the sending of the statistics.

When participating in Kaspersky Security Network (“KSN”), the Customer agrees to provide the following information:

- The unique software installation identifier;
- The full version of the installed software;
- The type identifier of the installed software;
- The unique identifier of the computer with the installed software.