kaspersky

Technical Support program for Premium and Premium Plus licenses

Term and conditions

kaspersky

1. General terms and conditions

Herein is given a list of technical support cases, in relation to which Kaspersky Lab will provide assistance to the owner of licenses for Kaspersky Lab products of Premium and Premium Plus types.

2. Definitions

«Company Account» – shall mean web-based Kaspersky Lab Technical Support request processing system (https://companyaccount.kaspersky.com).

«Product(s)» – shall mean software product(s) of Kaspersky Lab, which the Customer has purchased, deployed and installed in accordance with the terms of a License Agreement between Kaspersky Lab and the Customer, and for which the Customer has concluded a License Agreement.

«End User», «User»», «Customer», (You/ Your) – shall mean an organization, which has a functioning license to the Product that is suppose in accordance with a License Agreement.

«Technical Account Manager (TAM)» – shall mean a Kaspersky Lab technical support manager, performing as a personal technical manager for clients - Premium Plus license owners.

«Incident», «Request» – shall mean any event reported by the Customer, which is not part of the standard operation of a Product and which causes, or may cause, an interruption to, or a reduction in, the quality of service provided by the Product.

«Problem» – shall mean an unknown underlying cause of one or more Incidents. It becomes a Known Error when the root cause is known and a temporary workaround or permanent alternative has been identified.

«Known Error» – shall mean a Problem that becomes a Known Error when the root cause is known and a temporary workaround or permanent alternative has been identified.

«Product Error» – shall mean undeclared behavior of the Product.

«Service Request» – shall mean a request from a Customer for support, delivery, information, advice or documentation, which is not related to an incorrect functioning or non-functioning of the Product(s).

«Virus Outbreak» – shall mean a Customer crisis situation, where a virus undetected by the Product(s) with the latest antivirus bases and executable modules is affecting business continuity and/or a large number of Customer's end-users. Virus Outbreak is a product-related incident.

«Malware-related Incident / Virus Incident» – shall mean not product-related Incident, requiring Kaspersky to provide recommendations on particular malware removal, and/or malware descriptions, and/or special malware removal tools.

«Incident Severity/Urgency» – shall mean a measure of the business criticality of an Incident or Problem based on the business needs of the Customer.

«Response time» – shall mean the elapsed time measured from the moment of any Incident receipt till qualified answer to the initiator (via support system, email or phone).

«Update» – shall mean Kaspersky –issued anti-virus databases with new signatures or modifications of the Product's executable modules, which enhances its performance and/or expands its functionality.

«Workaround» – shall mean a procedure that may serve as a temporary solution to an incident.

«False Alarm», «False Positive» – shall mean a situation when the Product erroneously detects a safe file as an infected one.

kaspersky

3. Description of the support program

Requests receiving

Technical support relating to product operations as well as acceptance of post-incident maintenance requests, are implemented by the means of: support system, phone or email.

Web-portal

Kaspersky Company Account https://companyaccount.kaspersky.com – Kaspersky technical support web-portal with acceptance of requests 24x7x365 (around the clock, including weekends and holidays).

Phone

Priority telephone line is provided in the mode:

- 24x7x365 for Severity Level 1 and for Premium license owners;
- 24x7x365 for Severity Level 1 and 2, and for Premium Plus license owners;
- During business working hours (Local office time) for requests of Level 2, 3, 4.

Severity level of Incident	License type	
	Premium license	**Premium Plus license**
Level 1	24x7	24x7
Level 2	Business working hours	24x7
Level 3	Business working hours	Business working hours
Level 4	Business working hours	Business working hours

Business working hours may vary depending on the region, for more info check www.kaspersky.com

Email

Email acceptance of requests 24x7x365 (around the clock, including weekends and holidays if it is impossible to create a request through the Company Account.)

Incident processing incidents via web-portal

Web-based Kaspersky Technical support request processing system is available at:

https://companyaccount.kaspersky.com.

By the means of this system, Customer can take advantage of:

- access to personal account in order to create, update and monitoring incidents.
- technical support and consulting in relation to incidents that may occur during Product installation, configuration and functioning.
- technical support in relation to disinfecting files tampered by malware, as well as to removing malware from Customer's computers protected by the Products with latest anti-virus databases.

kaspersky

Processing incidents by phone

Technical Support by phone is only available to the authorized contact persons of the Customer.

Response times

Kaspersky guarantees the following response times, depending on the urgency of customer's request:

Severity level of Incident	Response time	
	Premium license	Premium Plus license
Level 1	2 hours*	30 minutes*
Level 2	6 working hours	4 hours*
Level 3	8 working hours	6 working hours
Level 4	10 working hours	8 working hours

*Phone call is requested during out of business hours incl. weekends and holidays

Requests from the customers of the Premium and Premium Plus licenses are assigned with higher priority compared to requests within the standard support package.

The urgency level is determined by the category chosen by the customer (using the drop down list in the Company Account) when contacting Technical Support and gist of the incident. Kaspersky reserve the right to revise the request's urgency level if the severity of the case as specified by the customer is not confirmed. The list of urgency levels with descriptions is provided in the Appendix.

Quality management

Incident escalation and claim management

Reclamations concerning quality of technical support are accepted according to the following scheme:

Escalation level	1	2
	Head of support team, Kaspersky Regional office	Business Account Manager (Business Contact)

Customer may escalate unresolved incidents in case it is currently on the Kaspersky side.

Incident resolution control

At any moment an incident can be either on the Customer's side (i.e. Customer is taking actions that will promote/expedite the resolution of the issue by Kaspersky) or on Kaspersky side.

An incident is on the Customer's side when Kaspersky requests information from the Customer. When Customer provides the requested information to Kaspersky Lab, the incident is considered to be on the side of the latter. The period during which the incident may be on the Customer's side is limited to 30 days. In case the Customer's response is overdue, the incident is closed by timeout.

Kaspersky is only responsible for the time during which the incident is on their side.

kaspersky

Anti-virus database release by customer's request on malware incident or false positive

In case of a false negative (when an infected file is identified by the Product as safe) or, oppositely, a false positive, on condition that the latest available anti-virus databases are utilized, Customer may request to make changes to anti-virus signatures of the Product. Kaspersky provides Customer with the update of the Product that will ensure correct detection of the file.

Kaspersky implements the following activities:

- Processing requests concerning anti-virus databases release (carried out by a dedicated group of specialists in a 24/7/365 mode)
- Release of high-priority (expedited) updates for the owners of Premium or Premium Plus licenses.
- Informing Customer about the progress of their requests by the means of Personal Technical Manager for the owners of the Premium Plus licenses.

Additional terms of support and benefits for the owners of the Premium Plus license.

Technical Account Manager (TAM)

Technical Account Manager (TAM) is assigned by Kaspersky in order to organize the only channel of interactions with the Customer. TAM is an employee of Kaspersky and manages processing of all customer incidents. The responsibilities of Technical Account Manager are determined as follows:

- organizing communications for processing incidents by Kaspersky technical teams:
- notifying Customer of the current status of incidents; providing quarterly reports;
- supervising the progress of tasks related to Customer requests and implementing timely escalations when processing requests;
- support of the Customer's IT department in relation to recommendations and instructions given by Kaspersky specialists;
- analytical working cooperation with the Customer in order to resolve current technical and operational incidents.

TAM is accessible during business working hours Monday to Friday from 10 a. m. till 6:30 p. m. (Kaspersky local office time) by landline phone, by cellular phone and by email. If the TAM is unavailable (Outside of normal business hours including weekends) the Customer's requests are directed to the manager-on-duty on the Technical Support line.

Customer assigns contact persons (in accordance to Additional terms of support) for communication with Kaspersky and TAM, and shares with the latter his or her contact details (email, telephone number and others if available) for consistent and efficient collaboration in connection with incident resolution.

Provision of reports on open incidents

During the process of incident resolution, Kaspersky will make every effort for promptly provide Customer with information on open incidents' status, according to the following table.

Severity level	Report schedule
Level 1	By agreement, but not more often than once a day (by email or by phone)
Level 2	Within the regular reports

Level 3	
Level 4	

Provision of the public and private patches

Kaspersky implements the following activities:

- Processing requests concerning the release of patches and private fixes (carried out by a group of engineers dedicated for Premium Plus license subscribers' requests)
- Informing Customer about the progress of their requests by the means of Technical Account Manager

Kaspersky will apply commercially reasonable efforts to release a private program correction code (private patch). Codes of program correction are released according to the product support lifecycle break down of the Support Service Terms and Conditions (an up-to-date version is available http://support.kaspersky.ru/support/rules)

The terms of using private program corrections are a subject of the License Agreement between Kaspersky and the Customer.

Additional terms of support

To register an incident, the Premium or Premium Plus license's owner should provide a list of contact persons who are entitled to make requests for technical support services.

The number of authorized persons varies depending on the type of license:

	Type of license	
	Premium license	**Premium Plus license**
Number of authorized persons	4	8

The list of contact persons should be determined and provided by the Customer to the Technical support at the first contact. To change the list of contact persons, the Customer should submit a request using the Company Account. In response to the request to change the list of contact persons Kaspersky will provide the User with an updated list of contacts.

Some incidents may require reproduction on Kaspersky side with the purpose of testing and verifying a virus infection or a product error.

Customer should provide Kaspersky with all information necessary and specific software or hardware, which may be necessary for reproducing the condition under which the incident will re-occur and could be examined. This may be needed if Kaspersky does not have the necessary software or hardware available.

Kaspersky will endeavor to reproduce the incident as soon as all of the necessary information and software and/or hardware is provided.

If the incident could not be reproduced, Customer should grant to Kaspersky specialists supervised remote access to the malfunctioning system.

kaspersky

Limitations of the technical support

Kaspersky has the right to refuse providing the level of service described in this support program if Product license is different from Premium or Premium Plus. It is forbidden to purchase different license types for the same Products. In such case, a Customer will be provided with support in accordance with the standard support package terms, posted on: https://support.kaspersky.com

Technical support covered by the Premium and Premium plus licenses shall not be implemented in case of the following incidents

- incidents already resolved for the Customer (i.e. incident that occurred on one installed copy of the Product after the same incident had been resolved for another copy of the Product);
- troubleshooting of all issues similar or identical to already resolved issues (i.e. the incidents to which a previously produced solution can be applied without additional guidance from Kaspersky);
- incidents caused by Customer's hardware malfunction;
- incidents caused by software platform incompatibility (including, but not limited to beta software, new versions of service packs or additions, whose compatibility with the Product has not been confirmed by Kaspersky);
- incidents caused by installing and running third-party applications (including, but not limited to the list of unsupported or incompatible applications published in the documentation);
- incidents for which the Customer cannot provide accurate information, as reasonably requested by Kaspersky, in order to reproduce, investigate, and resolve the incident;
- incidents which arise as a result of neglect or incorrect use of Kaspersky instructions, which, if properly used, would have obviously prevented the incident.

4. Appendix

Product incident severity levels

"Severity Level 1" (critical) shall mean a critical Product problem, which affects Customer's business continuity by interruptions in the Product's normal functioning and which causes the Product(s) or Operating System to crash, or which causes data loss, changing default settings to insecure values, or security issues, provided that there is no Workaround available.

The list of Product-related incidents, which refer to Severity Level 1, includes, but is not limited to, the following issues:

- all local network (or its critical part) is inoperative, which hampers or suspends core business processes.

"Severity Level 2" (high) shall mean a moderate issue which affects product functionality but does not cause data corruption/loss or software crash. Severity Level 1 is re-classified to Severity Level 2 when a workaround is available.

The list of Product-related incidents, which refer to Severity Level 2, includes, but is not limited to, the following issues:

- product malfunctions or does not function, but continuity of core business processes is not broken.

"Severity Level 3" (medium) shall mean a non-critical issue or service request, which does not affect Product's functionality.

The list of incidents, which refer to Severity Level 3, includes, but is not limited to, the following issues:

- product is partially out of service (malfunctions), but other applications utilized by the Customer are not involved.

"Severity Level 4" (minor) shall mean other non-critical issues or service requests. Al incidents that do not satisfy any of the above-listed criteria, refer to this severity level.

kaspersky

Virus incident severity levels

“Severity Level 1” (critical) shall mean virus outbreak, which affects Customer’s business continuity by interruptions in the Product’s normal functioning and which causes the Product(s) or Operating System(s) to crash, or which causes data loss, provided that there is no Workaround available.

The list of malware-related incidents, which refer to Severity Level 1, includes, but is not limited to, the following issues:

- all local network (or its critical part) is inoperative;
- virus outbreak;
- false positive for the files that refer to business-essential systems.

“Severity Level 2” (high) shall mean a moderate issue which affects product functionality but does not cause data corruption/loss or software crash. Severity Level 1 is re-classified to Severity Level 2 when a workaround is available.

The list of malware-related incidents, which refer to Severity Level 2, includes, but is not limited to, the following issues:

- infection of some non-critical network nodes;
- false positive for the files that do not refer to business-essential systems.

kaspersky

www.kaspersky.com/
www.securelist.com