kaspersky

Extended Technical Support Program for Technology Alliances (TA) products

MSA for Technology Alliances (MSA for TA)

kaspersky

1. General terms and conditions

This Support program defines the list and procedure for the provision of premium technical support to owner (Licensee) of Maintenance Service Agreement for Technical Alliances products (MSA for TA) certificate provided by Kaspersky (Licensor).

This Support program is intended to provide the Licensee with an extended scope of services, as well as enhanced quality of service over the Standard Support of the Technical Alliances products.

2. Definitions

"Company Account" – a web-system for processing incidents by the Kaspersky Technical Support (https://companyaccount.kaspersky.com)

“Licensee” – a company or organization which owes the Maintenance Service Agreement for Technical Alliances (MSA for TI).

“**Licensor”** – Kaspersky company.

"Incident" – any event reported by the Licensee, which is not part of the normal operation of the Product, and which causes or may cause interruption or reduction in quality of the service provided by the Product.

"Problem" – main unknown cause of one or more incidents. It becomes a known error when the root cause is known and a temporary workaround or permanent alternative is found.

"Known error"– a problem, whose root cause became known and a temporary workaround or permanent alternative was found.

"Product error"– undeclared behavior of the Product.

"Service Request" – a request from the Licensee for technical support, information, advice or documentation in cases not related to incorrect functioning or interruption of the normal operation of the Product.

"End User" – a client directly using the Licensee's Software containing the Product.

"Incident severity level"– a measure of how critical the incident is for business with respect to User's business needs.

“Malware outbreak” – a crisis situation on the End user’s side that occurs if malware cannot be detected by the Product using the latest anti-virus databases, and the executable modules of the malware affect the User's business continuity.

"Response time"– the time elapsed from the moment when the Licensor receives information about any incident until the moment when the Licensee receives a qualified response.

"Update" – the release of a database issued by the Licensor, which includes new signatures for malware detection or other Product modifications to ensure improved functionality or performance of the Product and/or to provide a new functionality or improvement of the Product.

“Workaround” – a procedure that may serve as a temporary solution to an incident for the Licensee.

kaspersky

3. End User Support (first line support)

The Licensee shall independently organize and provide Support to End Users (first line support), which includes:

- Consulting End Users on installation and use of the Product.
- Consulting End Users on update of databases and program modules of the Product.
- Diagnostics and fixing of problems that can be resolved independently.
- Diagnostics and fixing of known problems, the solution of which is described in the Product documentation and online resources.
- Diagnostics and fixing of problems similar to those resolved earlier.
- Initial investigation of problems that cannot be resolved independently.
- Obtaining information requested by the second line support.
- Implementation of solutions suggested by the second line support on the End User's side.
- Installation of Product updates on the End User's side.

4. Licensee Support (second line support)

The Licensor provides the Licensee with Technical Support (second line support), which includes diagnostics and solutions to problems occurring in process of the correct use of the Product in accordance with the documentation, which cannot be independently resolved by the first line support.

Support is provided via the following communication channels 24/7 (including weekends and holidays):

- Through the Company Account website (https://companyaccount.kaspersky.com)
- By email
- By phone (dedicated priority line)

When an incident is escalated to second line support, the Licensee shall provide the Licensor with the following information:

- The name and version of the Product used
- Detailed description of the problem
- Steps to reproduce the problem
- Configuration files of the Product (if any)
- Product logs (if any)

Some incidents may require replicating the conditions under which the problem occurred in order to test and verify a problematic scenario. In such case, the Licensee must provide the Licensor with all information and specific software or hardware necessary to reproduce the conditions of the incident.

The Licensor shall make every effort to reproduce the incident as soon as all the necessary information, software and/or hardware are available. If it is impossible to reproduce the conditions of the incident, the Licensee shall grant the Licensor's employees remote access to the systems where the problem is observed.

If the incident cannot be reproduced by any of the parties, or the client did not grant access to the work environment where the incident can be reproduced, or it has been established that the Product did not cause the incident, the Licensor has the right to refuse to perform any further works on the incident’s resolution.

kaspersky

Second line support limitations

Second line support does not support the following incidents:

- Incidents resolved earlier or similar to those resolved earlier.
- Incidents caused by hardware errors of the End User.
- Incidents that occurred in unsupported versions of program platforms (such as beta versions of program platforms, versions of new update or addition packages unapproved by the Licensor as compatible with the Product).
- Incidents caused by installation and execution of third-party applications (including, but not limited to the list of unsupported and incompatible software, stated in the documentation or on the Licensor's website).
- Incidents about which the Licensee cannot provide accurate information, reasonably requested by the Licensor to reproduce, analyze, and fix the incident.
- Incidents resulting from neglect or incorrect application of instructions or documentation of the Licensor, which, if applied correctly, would have made the incident impossible.

5. Incident response times

The Licensor guarantees the response time to the Licensee's requests in accordance with the periods for the respective incident severity level:

Incident severity level	Response time
Incident severity level 1	30 minutes*
Incident severity level 2	4 hours*
Incident severity level 3	6 working hours
Incident severity level 4	8 working hours

*During non-working hours the response time is guaranteed if the incident is additionally confirmed by the Licensee by phone call.

6. Dedicated Technical Account Manager (TAM)

A Dedicated Technical Account Manager (TAM) is appointed by the Licensor in order to organize a single communication channel for the Licensee. TAM is an employee of the Licensor who manages the processing of all incidents of the Licensee.

The responsibilities of a Dedicated Technical Account Manager include:

- Organization of works on Technical Support by the Licensor's specialists to resolve technical incidents
- Informing the Licensee about the current status of request resolution, providing quarterly reports
- Monitoring of task performance and ensuring timely escalation when handling incidents in the course of providing services
- Support for the Licensee's IT department in understanding and correct use of the recommendations, provided as part of services
- Conducting, together with the Licensee, regular analysis and coordination of actions necessary to resolve technical and operational incidents

The Licensee must provide the Licensor with the names and contact information of the employees assigned to interact with the TAM and provide the TAM's contact information (in particular, their email address and telephone

number), by which the contact person or authorized representative of such person can be contacted during the work on incidents.

The Licensee has access to a 24-hour dedicated technical support line.

7. Quality control

Incident escalation and claim management

Claims and complaints concerning quality of service shall be made according to the following scheme:

Escalation level	
1	Dedicated Technical Account Manager
2	Technology Product Support Team Lead
3	Corporate Account Manager (Business Contact)

Provision of reports on open incidents

In the process of resolving incidents, the Licensor shall make every effort to provide timely information on the status of open incidents to the Licensee in accordance with the schedule specified in the table below.

Incident level	Reporting schedule
Incident level 1	As agreed, but not more frequently than once a day (by e-mail or by phone)
Incident level 2	As part of the regular report
Incident level 3	
Incident level 4	

8. Additional support terms

The Licensee has the right to appoint up to 8 (eight) contact persons, entitled to initiate Technical Support requests. The list of Licensee's contact persons must be defined in the MSA certificate provided by Licensor. To change the list of contact persons, the Licensee must submit a request through the Company Account. In response to the request to change the list of contact persons, the Licensor will provide the User with an updated version of the Premium Technical Support certificate.

The User can register an unlimited number of incidents during the entire term of the Premium Technical Support certificate.

9. Incident severity levels

An incident severity level is determined based on the problem description provided by the Licensee when escalating to second line support. The Licensor has the right to subsequently reconsider the severity level if its description corresponds to a different level.

Premium Support requests are processed with a higher priority than standard requests.

"Incident severity level 1" (critical) means a critical Product problem that impacts the Licensee's business continuity by interrupting the operation of the Product or End User's operating systems, or causing data loss, changing default settings to an insecure mode, or other security issues, with no workaround available.
This includes the following malware incidents:

- The entire local network (or its critical part) does not function.
- Malware epidemic that affects the continuity of the End User's business by interrupting the operation of the Product or End User's operating systems, or causing data loss, with no workaround available.
- False alarm for files that are part of critical business systems.

Severity level 1 is re-classified to Severity level 2 when a workaround is available.

"Incident severity level 2" (high) means a problem of high severity that impacts the functionality of the Product, but does not cause data loss or damage, or interruption of software performance.
The list of incidents related to the Product and corresponding to severity level 2 includes the following incidents:

- The Product is inoperative, but the continuity of main business processes has not been interrupted

"Incident severity level 3" (medium) means a non-critical problem or service request that does not affect the Product functionality.
The list of incidents corresponding to severity level 3 includes the following:

- The Product is partially inoperative (it does not function correctly), but other software of the End User is not affected by the work of the Product.
- Infection of several non-critical network nodes.
- False alarm for files that are part of non-critical business systems.

"Incident severity level 4" (low) means other non-critical or service requests. All incidents not mentioned above fall under this severity level.

www.kaspersky.com/
www.securelist.com