

EXHIBIT D. SERVICE MODULE. INCIDENT RESPONSE

This Service Module sets out the special terms and conditions applicable to Kaspersky Incident Response Service and is to be read in conjunction with [Kaspersky Security Services Terms and Conditions](#).

General Terms and Conditions apply to this Service Module.

1. DEFINITIONS

“Attack” or “Cyber-attack” - any kind of activity for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure, Customers’ resources or destroying the integrity of the Customer data or stealing controlled information.

“Deliverable” – a report containing a description of the testing results and recommendations for further remediation actions. This stage of the Service is performed remotely or onsite, as agreed between Parties including via email or stated in Annex A of these T&Cs.

“Emergency Incident Response” – a format of the Service, provided in an emergency mode in accordance with the T&Cs and a related Scope of Work, if required.

“Incident” – a critical event or complex of events occurred in the Customers’ resources to be investigated by Kaspersky.

“Incident Response Retainer” – a format of the Service, provided on a subscription basis in accordance with the T&Cs, Order, and a certain Service Level Agreement.

“Kick-off call” – a call to be organized by the Customer and Kaspersky after the Effective Date. During the call, Parties representatives discuss details about the incident, suggest a Service delivery schedule (including business trips for onsite option, if needed), and request an additional information.

“Service” or “Incident Response” – an investigation service of Kaspersky aimed at producing a detailed picture of an incident. The Service covers the full incident investigation cycle from collection of evidence to identification of additional traces of compromise and preparing a remediation plan. The Service includes Digital Forensic and Malware analysis as described in this Exhibit D.

2. SERVICE DESCRIPTION

2.1. The goal of the Service is to get an independent expert analysis of incident evidence, to understand possible reasons, sources and impact of the Incident, and to plan remediation actions.

The following objectives are to be achieved during the execution of the Service:

- Stop spreading of the Incident, limit the damage and prevent further damage;
- Collection of evidence;
- Analyze evidence and reconstruct the Incident chronology and logic;
- Analyze malware used for the attack (if any malware found);

- Reveal the suspected sources of the attack and other compromised systems (if possible);
- Provide the tool and the identified IoC's to the Customer for scanning its infrastructure to reveal possible signs of compromise;
- Analyze outgoing connections from the Customer's network with external resources to detect suspicious ones (possible command and control servers);
- Provide recommendations on further remediation actions.

The following objectives are to be achieved during the execution of the **Digital Forensics**:

- Analyze evidence provided by the Customer and reconstruct the Incident history and logic;
- Analyze malware used for the attack (if any malware found);
- Reveal the suspected sources of the attack and other compromised systems (if possible);
- Provide recommendations on further remediation actions;
- For Kaspersky Endpoint protection clients - improve malware protection by adding the newly revealed malware to Kaspersky knowledge base (in case if the malware was found and was unknown before).

The goal of **Malware Analysis** is to understand how a specific piece of malware operates in order to build protection for the Customer's network. Malware Analysis is aimed to reveal ways of how a concrete machine was infected with this malware and its objectives.

The following objectives are to be achieved during execution of the **Malware Analysis**:

- Analyze malware sample;
- Provide recommendations on further remediation actions;
- For Kaspersky Endpoint protection clients - improve malware protection by adding the newly revealed malware to Kaspersky knowledge base (in case if the malware was found and was unknown before).

2.2. Report.

Findings are delivered in a detailed report covering:

- Time snapshot of an attack surface that was, is being or potentially could be exploited by cybercriminals for attacks against the Customer;
- Independent expert analysis of the Incident evidence to understand possible reasons, sources and impact of the Incident;
- Description of the sample and a verdict on its malware classification (in case if it is malicious);
- Information about malware activity on the infected machine;
- Suggestions for initial actions on the Incident response;
- Mitigation steps in accordance with the provided recommendations.

Report structure can vary depending on each Incident and the current scope of the Service.

3. SERVICE STAGES

3.1. The Service includes the following stages:

3.1.1. **Registration of Request.**

This stage applies to Incident Response Retainer. At this stage Customer submit the request with an incident description to a specified email. The request is registered and sent to Global Emergency Response Team. Concurrently Customer will receive confirmation that the request is accepted for processing.

3.1.2. **Start meeting.**

During this meeting, the project coordinator discusses the details of the Incident with the Customer's representative, proposes a schedule of Service to be carried out (including travel details, if onsite Service is required) and requests an additional information.

3.1.3. **Incident triage.**

Based on the information provided, Kaspersky conducts a preliminary assessment of the Service duration. The duration takes into account only the time actually spent on the provision of the Service, i.e., on:

- Kick-off meeting and follow-up communications;
- Analysis of the collected evidence;
- Reverse engineering of malware samples;
- Preparation of indicators of compromise for further scanning of the infrastructure;
- Identification of possible sources of attack and other suspected compromised systems (if possible);
- Development of the recommendations for eliminating the consequences of the Incident and implementing protective measures;
- Writing a final report on the results of the investigation.

Time spent by the Customer to collect and provide the evidence, as well as other similar Customer activities are not considered by Kaspersky in the estimated duration of the Service.

3.1.4. Initial response. This phase is focused on isolating the affected systems and preventing the Incident propagating further. Kaspersky will help to contain an Incident impact and prevent its spreading to other areas of the Customer's network. Containment measures allow to minimize Incident-caused damage and limit the potential further harm.

3.1.5. Data collection. Kaspersky implements best practices to accurately collect digital evidences necessary for a proper Incident investigation. Evidence may include: log files of operating systems, applications and network equipment, logs of Internet access (for example, from proxy servers), network traffic dumps, HDD images, memory dumps and any other types of information, which could be useful for investigation. Interviews with representatives of Customer and of any other

organizations involved into the Incident can also be organized. Access to monitoring systems (if they are used), such as SIEM, can be requested.

- **Onsite evidence collection by the Kaspersky.** Kaspersky visits the Customer's site and collect any type of evidence related to the Incident.
- **Evidence collection by the Customer.** In this case, the Customer collects all the evidence, and shares it with Kaspersky. Kaspersky will give recommendation and instructions that describes what kind of evidence to collect and how to collect it. Kaspersky will accomplish the forensic duplication task by using special software that collects drive images in a forensically-sound manner. Using these forensic tools, experts will analyze all relevant data on the system, including deleted files and unallocated areas on the disk.
- This stage of the Service is performed remotely/onsite.

3.1.6. Data analysis. At this stage Kaspersky performs analysis of all available information in order to recreate the picture of the Incident. This includes reviewing log files, system configuration files, trust relationships, web browser history files, email messages and their attachments, installed applications, graphic files, database transaction files, financial records, and countless other items. Kaspersky also performs software analysis, review time/date stamps, performs keyword searches, and completes any other necessary investigative steps required to understand the details of an Incident. Evidence analysis includes looking through information that has been logically deleted from the system to determine if deleted files, slack space, or free space contain data fragments or entire files that may be useful to resolve the Incident.

- In case if additional evidence is needed because of new discovered facts during the analysis, or if some information or access was not provided by the Customer during the first stage of the Service – the additional evidence can be collected by Kaspersky or delivered by the Customer remotely (via mail, e-mail or by providing remote access to certain systems, depending on the type of evidence).
- This stage of the Service is performed remotely.

3.1.7. Malware analysis (in case it was found). In order to understand how malware sample operates, Kaspersky will use Static and Dynamic analysis techniques.

- This stage of the Service is performed remotely.

3.1.8. Tool-aided scanning of network resources. If new indicators of compromise were built on the previous stage, Kaspersky provides the Customer with the tools and IOCs for scanning network resources to detect other compromised hosts.

- This stage of the Service is performed remotely.

3.1.9. Report preparation. At this stage, Kaspersky prepares a report containing a description of the investigation results and recommendations for further remediation actions.

- This stage of the Service is performed remotely
- 3.2. The Service is performed onsite/remotely, as agreed by Parties in written including via email, or as stated in the related Scope of Work.

4. DELIVERABLES

- 4.1. As a result of the Service Kaspersky prepares the report about the analyzed data and Incidents. The report includes the following information:
- **Executive summary** – brief description of the analysis conducted and of discovered threats to the Customer's resources.
 - **Detailed description** – an in-depth analysis of collected data, results of the initial Incident investigation, a description of exploited vulnerabilities and security flaws which could be used by malefactors, sources of any attacks and network resources which were affected.
 - **Remediation recommendations** – the report will suggest steps to mitigate consequences of the Incident occurred and to protect the Customer's resources from the similar attacks in future.

Any other reports, presentations, materials or other written information provided by Kaspersky as a result of the Service are Kaspersky Intellectual Property and will not be considered "Deliverables" as defined in the T&Cs.

Reports with investigation results are provided in English language.

5. OBLIGATIONS OF THE PARTIES

- 5.1. The Customer assumes the commitment to provide Kaspersky with all information and/or access to carry out the Service, and/or any additional resources, that may be reasonable required by Kaspersky. The Customer shall provide access to any additional resources which are necessary to perform the Service. When the Customer signs the SOW, if required by Kaspersky, the Customer will be deemed to explicitly authorize Kaspersky to perform the Service in accordance with the conditions, restrictions and guidelines set forth in the T&Cs.
- 5.2. Customer prior to Service performance must provide any resources to ensure no delays during the provision of the Service.
- 5.3. Kaspersky assumes the commitment to take all reasonable precautions in order not to impede correct functioning of the Customer's network resources.
- 5.4. Accordingly, the Customer shall:
- 5.4.1. notify Kaspersky of any matter(s) of which it is aware (or ought reasonably to be aware) which are reasonably likely to affect or relate to the performance of the Service, including in particular any known system defects, sensitive data or data for which a back-up and disaster recovery process has not been implemented;
 - 5.4.2. perform at its own cost any restoration or reparation work that may be required to restore functionality to the server functionality as a result of the Service;
 - 5.4.3. nominate times for the performance of the Service so as to minimize the potential for the Customer being adversely affected by the Service;

- 5.4.4.** release Kaspersky from any liability for any loss of production, loss of availability, loss of data, loss of connectivity, degradation of network bandwidth, loss of access to systems or loss of use suffered or incurred directly or indirectly by the Customer during Service provision;
 - 5.4.5.** co-operate with Kaspersky in all matters relating to the Service and provide in a prompt manner, any information, documents, or materials which may reasonably be required by Kaspersky to deliver the Service and, in relation to any information provided, ensure that such information is complete and accurate in all material respects;
 - 5.4.6.** not initiate or recommend any law enforcement or civil lawsuits against Kaspersky in response to the Service performance. In the event of any law enforcement or civil action brought by anyone other than Customer, Customer will take steps to make known, either to the public or to the court, that these activities were conducted pursuant to and in compliance with these T&Cs and constitute as authorized by the Customer;
 - 5.4.7.** ensure to revoke all access permissions given to Kaspersky during the Service delivery after final report is provided as well as roll back all configuration changes implemented for the purpose of the Service provision.
- 5.5.** Accordingly, Kaspersky will:
- 5.5.1.** perform the Service remotely and/or onsite, as agreed in writing including via email or stated in the related SOW;
 - 5.5.2.** deliver the Service or, if applicable, each part of the Service on the Service Delivery Date set out in the related SOW unless otherwise agreed in writing between Kaspersky and the Customer;
 - 5.5.3.** use its reasonable endeavors to meet any agreed deadlines for completion of the Service;
 - 5.5.4.** use reasonable efforts and take reasonable precautions when performing the Service.

6. LIABILITY LIMIT

- 6.1.** Customer acknowledges that Kaspersky ability to provide the Service and to meet any timeframe agreed for the provision of the Service is dependent on the Customer providing that information and access to and facilities and equipment providing decisions and instructions at the times required by Kaspersky.
- 6.2.** The Customer confirms that reverse engineering of any binaries provided to Kaspersky does not infringe any rights of third parties or violate any applicable laws.
- 6.3.** Kaspersky does not provide in-depth analysis of malware samples detected on the Customer's resources, if the malware is not related to the current Incident, unless this Malware Analysis specified in the initial request.
- 6.4.** The Customer assumes the commitment to provide Kaspersky with all required information and/or access to carry out the analysis, and to cooperate with Kaspersky team involved in the Incident resolution. The Customer shall provide access to additional resources which

necessary to analyze or recreate conditions of Incident emergence (if Kaspersky does not have the necessary software and/or hardware). Kaspersky is not liable for completeness and accuracy of investigation results, if the provided data is incomplete, distorted or the provided information could not be analyzed due to lack of necessary technical means (such as rare hardware/software).

- 6.5.** The Customer agrees, that if additional evidence is provided after completion of the onsite evidence collection stage (either because information or access was not provided earlier, or because new evidence was requested by Kaspersky based on new facts revealed during the evidence analysis stage), then the Service can be extended on the duration of the additional evidence collection and analysis (the latter is as estimated by Kaspersky).
- 6.6.** The Customer realizes that reconstruction of a full picture of the Incident, as well as developing recommendations allowing to completely restore the Customer's resources may be impossible, depending on the Incident and available evidence.
- 6.7.** The Customer realizes that the goal of the Service is to understand possible reasons of the Incident (possible attack vectors in case if the Incident was a result of an intentional attack) and effectively plan mitigation actions, so investigation activities are performed to the extent enough to achieve this goal. Deeper investigation (such as identification of persons or groups of people being sources of the Incident) is out of the Service scope.
- 6.8.** Kaspersky assumes the commitment to take all reasonable precautions to in order not to impede correct functioning of the Customer's network resources.
- 6.9.** Each request of the Incident Response Retainer service will be charged for minimum of eight (8) hours.
 - 6.9.1.** One (1) case is limited by one-hundred and twenty (120) hours for the customers, whose IRR model includes number of cases instead of hours. Exceeding of this limitation will be charged as two (2) cases. Two false-positive requests will be charged as one (1) case.
- 6.10.** The Service is vendor agnostic, means that its performance does not require: i) Kaspersky products installed in the Customer infrastructure, (ii) use of any Customers' solutions.
- 6.11.** Kaspersky reserves the right to choose any software for the Service provision.
- 6.12.** Reaction time described in the Service Level Agreement section can be fulfilled for two (2) cases requested at the same time. Further cases will be handled to with the best efforts of the Service Level Agreement.
- 6.13.** In the event that performance of the Service is delayed or otherwise adversely affected by the failure of the Customer to meet its obligations, Kaspersky shall bear no responsibility for such delay or other consequence arising from the Customer's failure to act.
- 6.14.** If the Service at the Customers' premises is delayed due to circumstances which are not the liability of Kaspersky, the Customer must bear the reasonable cost of waiting time and any additional traveling expenses incurred by Kaspersky personnel.
- 6.15.** By entering into these T&Cs, Customer acknowledges and agrees that any remote part of the Service will be performed from the multiple locations and resources under Kaspersky control that may change and may not be explicitly registered to Kaspersky.

- 6.16.** The Service will be limited by the time available, scope of activities, as detailed in the related SOW, if required, unless otherwise agreed in writing between Kaspersky and the Customer, and information made available to Kaspersky, and Kaspersky does not covenant, guarantee or warrant to reveal all cybersecurity threats existing in the Customer information systems/resources, and Kaspersky shall not be liable for any consequences occurred due to damage caused by cybersecurity threats and consequently the Deliverables, produced as a result of Service should not be relied upon as a comprehensive record of such attacks.
- 6.17.** Customer understands and acknowledges that no use of or connection to the Internet is absolutely secure and Kaspersky is not liable for any loss, damage or adverse consequences suffered by the Customer whatsoever resulting from use of or connection to the Internet, including unauthorized access to, damage or loss of the Deliverables, information or other materials to be transmitted between the Parties.
- 6.18.** Customer agrees that the Service will be provided by Kaspersky group of companies.

7. SERVICE LEVEL AGREEMENT

This section applies to Incident Response Retainer.

Type of engagement	Triage SLA	Response SLA
Onsite	24 hours	24 hours
Remote	2 hours	8 hours

Triage SLA. The time to process and take request into work.

Response SLA. Initial data analysis and providing the Customer with an interim result.

Remote/Onsite works. Section 3 describes stages that can be performed remotely/onsite.

The Service is carried 24x7.

8. REPURPOSING RULES

These rules apply to the Incident Response Retainer only.

- 8.1.** Customer has right to apply 50% of the Service cost or from forty (40) to eighty (80) of the purchased hours in case if the Service was not used during the Period of Service Provision, to the following Kaspersky services (services composition may be changed by Kaspersky):
- [Kaspersky xTrainings](#)
 - [Kaspersky Compromise Assessment](#)
 - [Kaspersky SOC Consulting](#)
 - [Kaspersky Managed Detection and Response](#)
- 8.2.** Customer may contact its account manager to repurpose the unutilized Service. New Order shall be placed within thirty (30) days after the expiration date of the Period.

9. GENERAL

- 9.1. Customer agrees that it shall be solely responsible for the management, conduct and operation of its business and affairs, including without limitation for deciding on its use of the Deliverables, choosing to what extent it wishes to rely on the Deliverables, and/or implementing the Deliverables.
- 9.2. Customer warrants and represents that all of its resources are allocated exclusively to Customer and under the Customer's exclusive control.
- 9.3. Customer warrants that where its resources, required for the Service performance are not allocated exclusively to the Customer and under the Customer's exclusive control, Customer have obtained the express consent of the registered owner for Kaspersky to carry out the Services against all resources, and Customer shall indemnify Kaspersky in the event that the registered owner brings any claim against Kaspersky.
- 9.4. Customer agrees that the T&Cs apply from the Effective Date.

10. CONDITIONS REGARDING PERSONAL DATA PROCESSING

- 10.1. This section only applies where personal data is transferred and processed in accordance with the relevant legislations.
- 10.2. Under this section the following additional definition is introduced:

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Subject means a natural person which personal data may be processed by providing of the Service, including a representative of the customer, contractor, employee, client of the Customer, or other persons, in respect of whom data is transmitted and processed in the context of the Customer's activities, including data which may represent personal data under the laws of certain countries.

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Swiss FADP means the Swiss Federal Act on Data Protection of 19 June 1992 and its corresponding ordinances, in each case, as may be amended, superseded, or replaced.

DPA UK means Data Protection Act, 2018 of the United Kingdom.

UK Addendum means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the Information Commissioner under S119A Data Protection Act 2018, which can be found at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance>.

- 10.3.** In accordance with all applicable EU Data Protection Laws, BRAZILIAN GENERAL DATA PROTECTION LAW (LGPD) and other applicable laws, Customer shall be the data Controller and Kaspersky shall be the data processor, processing data on Customer's behalf.
- 10.4.** The following provisions shall apply to the extent that: (i) Customer is located in the European Union/European Economic Area, UK or Switzerland; or (ii) is located outside of the European Union/European Economic Area, UK or Switzerland but remains subject to the GDPR, Data Protection Act 2018 (UK GDPR) or Federal Act on Data Protection (Swiss FADP).

The Parties hereby conclude the data processing agreement, attached to the relevant Scope of Work and forming part of the conditions.

In case of processing of Controller Data involves transfer of personal data to the country outside EU for which there is no adequacy decision or appropriate safeguards to ensure an adequate level of protection of the data equivalent to the EU, the Parties hereby conclude the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Commission Implementing Decision (EU) 2021/914 of 4 June 2021) in the version agreed by the parties.

For the avoidance of doubt, should the transfer mechanism based on standard contractual clauses be deemed invalid by a Supervisory Authority or court with applicable authority, the Parties shall endeavor in good faith to negotiate an alternative mechanism (if available and required) to permit the continued transfer of Personal Data.

- 10.5.** Pursuant to the Federal Data Protection and Information Commissioner's (FDPIC) guidance titled "The transfer of personal data to a country with an inadequate level of data protection based on recognized standard contractual clauses and model contracts", dated 27 August 2021, the parties are adopting the GDPR standard for all data transfers under the Swiss FADP and under the GDPR. To the extent personal data is transferred outside of Switzerland to a country with an inadequate level of data protection, the following amendments to the Standard Contractual Clauses shall apply:
- Annex I.C: The competent supervisory authority shall be the FDPIC, insofar as the data transfer is governed by the Swiss FADP; and shall be the EU authority referenced in Annex I.C insofar as the data transfer is governed by the GDPR.
 - The term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c).
- 10.6.** For Customers and/or Data Subjects who are residents of the United Kingdom, Kaspersky shall, where applicable:

(a) provide its Services in accordance with its obligations under the UK Addendum, which is incorporated into this DPA by reference; and

(b) as required by applicable law, transfer and process Personal Data on the basis of the Standard Contractual Clauses, as modified in accordance with the UK Addendum.

The UK addendum shall be structured as follows: (i) Table 1 shall be populated by the information in Annex I of the DPA attached to this T&C; (ii) Table 2 shall be populated by the information in the DPA attached to this T&C; (iii) Table 3 shall be populated by Annexes I – III

of the DPA attached to this T&C; and (iv) in Table 4, either the Importer or the Exporter may terminate this Addendum.

- 10.7.** For Customers and/or Data Subjects who are residents of the Federal Republic of Brazil, Kaspersky shall, where applicable: (a) provide its Services under the express obligations imposed by the LGPD on a Data Processor for the benefit of a Data Controller; and (b) as required under Articles 33 through 36 of the LGPD, transfer Personal Data on the basis of the Standard Contractual Clauses, as modified in accordance with the LGPD.
- 10.8.** The Customer authorizes Kaspersky to anonymize event data processed during the Service provision. "Anonymized Data" refers to information derived from the Customer Data, that has been irreversibly transformed such that it no longer relates to an identified or identifiable natural person, Customer, account, device, or system resource, rendering re-identification impossible by any party using reasonably available means. Kaspersky may retain and use Anonymized Data during and after the term of these T&Cs solely to maintain, test, and improve the Service, including enhancing threat detection algorithms and analytical models. Anonymized Data shall not contain Confidential Information, shall not be considered Personal Data or Customer Data, and falls outside the scope of confidentiality and processing restrictions under these T&Cs.

11. APPLICABLE LEGISLATION

- 11.1.** The Customer confirms the carrying out of the Service does not contravene any law or regulation, in particular as it relates to individuals, users, third-party information stakeholders, third-party information service providers or other parties likely to be affected by the Service on the Customer's information systems.
- 11.2.** For the purposes of the Computer Misuse Act 1990 (or any statutory modification or reenactment or foreign equivalent thereof) the Customer consents to Kaspersky accessing and assessing its IT systems and networks (including without limitation any programs or data held on such systems and networks) to enable Kaspersky to provide the Service.
- 11.3.** For the purposes of applicable copyright legislation, the Customer grants the rights to evaluate, alter, and/or circumvent technical and/or security measures of the Customer's resources, IT infrastructure, and data, where necessary for the Service performance.