

## EXHIBITS A. SERVICE MODULE. APPLICATION SECURITY ASSESSMENT

This Service Module sets out the special terms and conditions applicable to Kaspersky Application Security Assessment Services 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

**“Scope of Work”** - the details of Customers applications, URL or any other resource are given in Annex A of this T&C. Services will be performed for the applications stated in Annex A unless explicitly agreed with the Customer by other means.

**“Services”** - security assessment of one or multiple applications, as stated in Annex A - “Scope of Work” performed by Kaspersky security experts in accordance with Kaspersky application security assessment methodology.

**“Deliverable”** - report containing detailed technical information on the assessment processes, results and identified vulnerabilities along with corresponding remediation recommendations.

### 2. OBLIGATIONS OF THE PARTIES

- 2.1. Customer acknowledges that, in providing the Services, Kaspersky will access Customer assets, including, but not limited to applications, related infrastructure and data. Customer will secure in advance of commencement of Services all permissions, consents or authorizations necessary for Kaspersky to access and use such Customer Application and data to perform Services under this T&C and/or the Direct Agreement, and/or to use any third-party Application (s) or data Kaspersky may use or require access to in performing the Services. When the Customer signs the SOW, the Customer will be deemed to explicitly authorize Kaspersky to perform the Services and conduct security research and vulnerability disclosure activities in accordance with the restrictions and guidelines set forth in SOW.
- 2.2. Customer represents and warrants that no object on which Services are to be performed is a critical infrastructure or part thereof or deemed as such under law, including systems or assets, whether physical or virtual, that are essential for the proper functioning of society and economy, and the incapacity of which would have a debilitating impact on security, national economic security, public health or safety, or combination thereof.
- 2.3. Customer acknowledges that Kaspersky ability to provide the Services and to meet any timeframe agreed for the provision of the Services 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.
- 2.4. Customer acknowledges the risks and the limitations of the security assessment which Customer accepts and is responsible for managing. Accordingly, the Customer shall:
  - 2.4.1. obtain appropriate consents from its internet service providers, hosting providers and any third-party owners/licensors of the parts of the Customer’s application to be tested during Services delivery;



to the target applications, denial of access to a legitimate system user, automatic shut-down of information systems or failure of the information system.

### 3. LIABILITY LIMIT

- 3.1. Actions, required for provision of Services, which may lead to denial of services shall be preliminarily negotiated with a Customer's representative. If any software failures occurs during the assessment due to security checks, Kaspersky will inform the Customer and provide detailed information about the actions taken.
- 3.2. In case of technical issues arise, which hamper the testing process including ones caused by manual or automated intrusion detection and response procedures (lack of network access to the tested resources, blocking of the service provider's IP addresses or accounts, etc.), the Customer shall resolve the issues in case if the problem is on the Customer's side. In such cases, the corresponding test and potential attack vectors are not considered during further testing, or the Services schedule is modified in accordance with the duration of delay in access.
- 3.3. In the event that performance of the Services is delayed or otherwise adversely affected by the failure of Customer to meet its obligations, Kaspersky shall bear no responsibility for such delay or other consequence arising from the Customer's failure to act.
- 3.4. By entering into this T&C, Customer acknowledges and agrees that any remote security assessment will be performed from multiple locations and assets under Kaspersky control that may change and may not be obviously registered to Kaspersky.
- 3.5. Services will be limited by the time available, scope of testing, as detailed in the related SOW and information made available to Kaspersky, and Kaspersky does not covenant, guarantee or warrant that the Services will detect all existing or potential vulnerabilities in the systems or applications within the agreed testing scope and consequently the Deliverables, produced as a result of Services should not be relied upon as a comprehensive record of such vulnerabilities. Service Deliverables, produced by Kaspersky, provide a "snapshot" of security posture of analyzed system or application taken at the identified point in time.
- 3.6. 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 Customer whatsoever resulting from use of or connection to the Internet, including unauthorized access to, damage or loss of the Deliverables or any source code, information or other materials to be transmitted between the Parties.

### 4. GENERAL

- 4.1. 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.
- 4.2. Customer acknowledges that Kaspersky uses the same tactics, techniques and procedures as real world attackers and shall notify its information and security teams as necessary that there may be an increase in logging activity and an increase in any intrusion detection or prevention system alerts during the Period of the Services Provision.

- 4.3. Customer prior to such Services performance must provide any resources (such as VPN access, IP whitelisting, etc.) to ensure no delays during the provision of the Services.
- 4.4. Customer warrants and represents that either each of the systems listed in the related SOW is allocated exclusively to Customer and is under Customer's exclusive control.
- 4.5. Customer warrants that where the applications listed in SOW are not allocated exclusively to the Customer and under Customer's exclusive control, Customer have obtained the express consent of the registered owner for Kaspersky to carry out the Services against each application. The registered owner has acknowledged that it is possible that the provision of the Services could cause disruption to applications and Customer shall indemnify Kaspersky in the event that the registered owner brings any claim against Kaspersky.
- 4.6. Customer agrees that the T&C applies retrospectively from the Service Delivery Date of the Services.
- 4.7. Customer confirms and agrees, that its publicly available policy, relating to conducting vulnerability research or bug bounty policy, is not applicable in respect to the Services.

## 5. CANCELLATION FEES

- 5.1. Kaspersky is entitled to an extension of time to perform its obligations under this T&C, which is equal to the delay caused by the Customer, without prejudice to any other right or remedy it may have, in cases if Kaspersky performance of its obligations under this T&C is prevented or delayed by any act or omission of the Customer (including but not limited to failure to provide access/access prolongation to the Customer's premises or facilities where required, failure to provide required data, information and credentials within reasonable time to commence the Services, not scheduling or participating in required events, etc.). In such circumstances Kaspersky has no liability in respect of such delay in the provision of the Services and may invoice Customer directly or through the Partner for any additional charges incurred in relation of the said extensions.
- 5.2. In the event that the Customer cancels the Services prior to the agreed Service Delivery Date or requires the Service Delivery Date to be changed at short notice then the Customer shall make such cancellation or change to the Service Delivery Date in writing to Kaspersky.
- 5.3. In the event that the Customer reschedules or cancels the Services prior to the Service Delivery Date, Kaspersky may, at its discretion charge the Customer a late cancellation fee and recover any out-of-pocket expenses incurred as a result of the cancellation or rescheduling of the Services. The cancellation fee shall be calculated as a percentage of the services fees that correspond to the days scheduled by Kaspersky for provision of the Services.
- 5.4. The relevant percentages and time periods of cancellation or rescheduling fees are set out in below:
  - 5.4.1. A cancellation or rescheduling request received in writing between five-fifteen (5- 15) Business Days before the Service Delivery Date: 50% of the service fee, stated in the invoice, provided by Kaspersky or the Partner to Customer, and
  - 5.4.2. A cancellation or rescheduling request received in writing within five (5) Business Days of the Service Delivery Date: 100% of the service fee, stated in the invoice, provided by Kaspersky or the Partner to Customer.

- 5.5. Kaspersky reserves the right to charge for the provision of Services carried out outside Business Days that is either requested by the Customer or necessitated due to the Customer's failure to perform its obligations. This will be charged at an individual rate set out in the Proposal and/or in the SOW.
- 5.6. Customer accepts and acknowledges that Kaspersky allocates its experts weeks or months in advance and would suffer a loss should the Services or any Services part be postponed or cancelled at short notice. As such, Customer agrees that it shall pay to Kaspersky (as genuinely pre-estimated liquidated damages) an amount to reflect the losses which Kaspersky will incur if such cancellation or rescheduling is requested within a set number of Business Days of the Service Delivery Date.

## 6. APPLICABLE LEGISLATION

- 6.1. Customer confirms the carrying out of the Services 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 Services on the Customer's information systems.
- 6.2. For the purposes of the Computer Misuse Act 1990 (or any statutory modification or reenactment or foreign equivalent thereof) 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 Services.
- 6.3. For the purposes of applicable copyright legislation, Customer grants rights to evaluate, alter, and/or circumvent technical and/or security measures of the Customer's applications, IT infrastructure, and data, where necessary for the performance the Services.