TERMS AND CONDITIONS

KASPERSKY APPLICATION SECURITY ASSESSMENT SERVICE

WHEREAS, the Customer named in the corresponding order ("Customer") desires to acquire the Kaspersky Application Security Assessment Service ("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 goal of the service is to obtain independent assessment of the current web applications security posture and evaluate effectiveness of implemented security controls.

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

- Reveal security flaws in the web applications
- Assess vulnerabilities’ severity and related possible impact
- Demonstrate exploitation of the most critical vulnerabilities
- Provide recommendations to fix the detected vulnerabilities

Service Options:

For web application security assessment our experts use black-box, grey-box and white-box approaches:

- Black-box – assessment without user credentials to reveal vulnerabilities available for an external attacker without any privileges.
  
  Duration: 10 business days for security assessment, 10 business days for report preparation
  
  Total Duration: 20 days

- Grey-box – revealing vulnerabilities available to authenticated users. Test user accounts must be provided for analysis.
Duration: 15 business days for security assessment, 10 business days for report preparation
Total Duration: 25 days

- White-box – source code and architecture analysis. Additional usage of white-box security assessment allows revealing a maximum possible amount of vulnerabilities in an application. To provide the most accurate results white-box assessment is used only with black-box and grey-box, which allows to verify detected vulnerabilities.

Duration: 15 business days for security assessment, 10 business days for report preparation
Total Duration: 25 days

Durations are calculated for the security assessment of 1 application
Duration may be increased if delays occur in provision of the access to the application and other arrangements from the Customer side
Duration may be increased in cases when application has a very complex logic

Approach and methodology:
Security assessment is performed in accordance with Kaspersky Lab’s own methodology based on international standards and best practices, such as standards and guidelines provided by:
- Open Web Application Security Project (OWASP)
- Web Application Security Consortium (WASC)

The analysis is performed both using automated tools and manually by experts. The following main security assessment tools will be used:
- Various general-purpose and specialized application scanners (Nessus, Acunetics WVS, NMap, and others)
- Source code analysis tools
- Specialized solutions for web application security assessment (OWASP dirbuster, BurpSuite, ProxyStrike, various plug-ins for Mozilla Firefox)
- Complex security assessment solutions (Kali Linux)
- Various web browsers (including old versions) to analyze client-side attacks
- And others

Confidentiality, integrity and availability of Customer’s applications are our top priority. Kaspersky Lab’s experts will take all necessary precautions to avoid any harm to Customer’s environment. The white-box approach (source code analysis without access to the applications) will be used as a basis, while dynamic methods (black-box and grey-box) will be mainly used for verification of found vulnerabilities. All sensitive technical information related to the project (source codes, credentials, assessment results, etc.) will be stored and transferred with usage of strong encryption, and can be removed upon Customer’s request after completion of the project.
The project team members are experienced professionals in web application security having deep knowledge in this field, constantly improving their skills, and acknowledged by industry leaders for their security research, such as Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens, SAP, and others (see section 7 for description of the project team).

**Outcome:**

By following the approach described above Kaspersky Lab will be able to reveal the following types of vulnerabilities in Customer’s applications:

- Absent or insufficient authentication and authorization
- Code injection (SQL Injection, OS Commanding, etc.)
- Vulnerabilities in the applications’ logic, which could be used for fraud
- Mistakes in the implementation of application functions available to a user
- Vulnerabilities leading to direct access to system objects (Path Traversal, etc.)
- Client-side vulnerabilities (Cross-Site Scripting, Cross-Site Request Forgery, etc.)
- Insecure data storage, including lack of encryption
- Insufficient entropy of important parameters, such as session identifiers or one-time passwords, leading to possible guessing by an attacker
- Information disclosure, including information about the specifics of application functions’ implementation and program components used, as well as other information that can be used by an intruder to develop an attack
- Improper configuration of an operating system, a web server, and other components
- And other application vulnerabilities including ones leading to the threats listed in WASC Threat Classification v2.0 and OWASP Top Ten

As a result of the project the Customer will obtain a report containing the following:

- Conclusions on the current security posture of the analyzed applications (including description of possible threats)
- Description of the project scope
- Description of the methodologies and tools used
- Description of the found vulnerabilities, information about their severity levels, exploitation conditions and complexity, and related impact
- Demonstration of vulnerabilities exploitation (for the most critical ones)
- Recommendations on elimination of vulnerabilities or implementing compensative controls
- A resulting list of detected vulnerabilities and corresponding recommendations for every application

**2. SERVICE DELIVERY**
2.1. **Conditions.** The Service is provided remotely.

2.2. **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.

2.3. **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.

2.4. **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.

2.5. **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 EXPLICITLY SET FORTH HEREIN, 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.

2.6. **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.

2.7. 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 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.

4. Liability Limit

4.1. Kaspersky Lab assumes the commitment to take all reasonable precautions in order not to impede correct functioning of the Customer's network resources.

4.2. Actions which may lead to denial of service shall be preliminarily negotiated with a Customer representative. Such actions shall be conducted on condition of the on-site presence of a Customer's employee responsible for the project. If any hardware or software failures occur during testing, the Kaspersky Lab shall inform the Customer about the incident and provide advisory help in its elimination.

4.3. By agreeing with the execution of the works, the Customer takes the risk of possible negative consequences of the tests. Considering that some tests completely simulate malicious attacks, the Customer undertakes the obligation to resolve potential disputes related to claims of Internet service providers or any other legal entities and individuals against Kaspersky Lab.

4.4. The Customer is aware that during black-box and grey-box security assessment availability of services and applications can be reduced and stored data can be partially modified. The Customer assumes a commitment to settle the potential problems arisen in this connection, and shall not raise any claims against the Kaspersky Lab for these reasons.

4.5. In case of technical issues arise which hamper the testing process including ones caused by prevention security systems (lack of network access to the tested resources, blocking of the Kaspersky Lab’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
attack vectors are not considered during further testing, or the project schedule is postponed for the duration of delay in access.