onecom

Onecom CyberProtect Service Terms

1 General

These Onecom CyberProtect Service Terms should be read in conjunction with all other terms of the Contract.

2 Interpretation

2.1 Terms defined elsewhere in the Contract shall have the same meaning in these Onecom CyberProtect Service Terms. The following definition shall also apply:

EULA	the end user licence agreement between Onecom and the Customer, a copy of which can be found at https://onecomcyberprotect.com/eula, as may be amended from time to time
Planned Maintenance Hours	the period between 10pm and 6am UK time
Software	the online software applications for dark web monitoring and digital attack surface analysis (and such other functionality, if any, that may be available from time to time)

2.2 The rules of interpretation set out in the General Terms shall apply to these Onecom CyberProtect Service Terms.

3 Service overview

3.1 Onecom CyberProtect is an online hosted service providing dark web monitoring and digital attack surface analysis to detect whether sensitive information, confidential Information and/or Personal Data has been compromised and the risk of a potential digital attack or online exposure.

3.2 As part of the Service, Customer data will be matched with publicly available information collected from the dark web to determine whether the Customer's data has been exposed, stolen or compromised. As such, Onecom and the Customer will be solely responsible for selecting the data that Onecom or the Customer wishes to be entered into the Service, and which Onecom and/or the Customer wants to (a) monitor from being exposed on the dark web, and (b) be notified/alerted in the event of Onecom or the Customers data being exposed/discovered on the dark web.

3.3 Information is collected and accessed from the dark web:

3.3.1 by taking the necessary precautions, including the use of an encrypted connection and virtual private network;

3.3.2 using legitimate credentials as provided by the dark web forums operators;

3.3.3 solely for the purposes of providing the Service to the Customer;

3.3.4 for legitimate cybersecurity purposes (e.g., to help identify cybersecurity threats); and

3.3.5 with no criminal, fraudulent or malicious intent or motive.

3.4 The information collected and accessed from the dark web is information that has expressly been stolen and/or exposed and is intended by the dark web forums or sites or systems to be made available/accessible to the public.

3.5 No stolen information that is exposed/discovered on the dark web from any third party is purchased as part of the Service.

3.6 The Service will be configured, delivered and managed remotely.

4 EULA

4.1 The Customer agrees and accepts that it is a condition of using the Service that the Customer agrees and enters into the EULA.

4.2 The Customer shall procure that all Users comply with the terms of the EULA.

4.3 The Customer shall immediately notify Onecom if it becomes aware of, or reasonably expects, that a User has breached the terms of the EULA.

4.4 No variation of the terms of the EULA will be effective unless it is agreed in writing.

5 Customer obligations

5.1 The Customer shall not

5.1.1 under any circumstances, attempt to circumvent or interfere with the security features of the Software;

5.1.2 reverse engineer, disassemble, decompile to human-perceivable form all or any part of the Software, or attempt to do the same;

5.1.3 the Customer shall not use any data, reports, analyses, statistics or other information obtained from the use of the Service for the purposes of verifying or evaluating (a) any third party's credit worthiness or personal, family or household insurance needs; (b) any third party's employment, promotion, reassignment or retention as an employee, as applicable. As such, the Customer agrees that it shall not use any data, reports, analyses, statistics or other information obtained from the use of the Service for improving or providing advice to any third party in relation to the third party's credit record, credit history or credit rating.

5.2 The Customer shall:

5.2.1 use sufficiently strong passwords for accessing the Service, keep such passwords secure and confidential and not disclose any passwords to third parties;

5.2.2 comply with Onecom's reasonable and lawful instructions as notified to the Customer from time to time;

5.2.3 only use the Service for the purpose of protecting the Customer's business/personal interests, to perform penetration tests or for ethical hacking purposes;

5.2.4 ensure that any user viewing the data has authority to view it and shall not use it for criminal activity or onward sharing;

5.2.5 only use the Service in accordance with all applicable laws and regulations and not knowingly do or omit to do anything which would put Onecom in breach of any such laws or regulations.

5.3 The Service is supplemental to, and is not intended to replace, any physical, technical, or procedural security measures (including but not limited to filters, virus software, firewalls, surveillance or information security programs) that the Customer may now have or implement in the future. The Customer acknowledges and understands that no security solution can be one hundred percent (100%) effective, and as such by using the Service no guarantee is given regarding the quality, effectiveness, or efficiency of the Customer's security framework/posture, including any policies, procedures, or operations or the accuracy of the Service.

5.4 The Customer acknowledges that no liability or obligation is accepted by Onecom (howsoever arising whether under contract, tort, in negligence or otherwise):

5.4.1 that the Software shall meet any Customer's (or other person's) individual needs, whether or not such needs have been communicated to Onecom;

5.4.2 that the operation of the Software shall not be subject to minor errors or defects; and

5.4.3 that the Software shall be compatible with any software or with any particular hardware or equipment other than as set out in this Agreement.

5.5 The Customer acknowledges and accepts that all warranties, conditions, terms, undertakings or obligations of Onecom whether express or implied and including any implied terms relating to quality, fitness for any particular purpose, reasonable care and skill or ability to achieve a particular result are excluded to the fullest extent allowed by applicable law.

6 Proprietary Rights

No Intellectual Property Rights are granted to the Customer, or any other rights or licences by these Onecom CyberProtect Service Terms.

7 Service Availability

A service availability service level of 99% applies to the Service.

8 Onecom obligations

8.1 Onecom will use commercially reasonable endeavours to provide the Service in keeping with the service availability set out at clause 7 but gives no warranty or guarantee in this respect.

8.2 Onecom with provide support services via (i) telephone and chatbot during Business Hours Monday to Friday, and (ii) ticketing system, twenty-four hours a day seven days a week (24/7), in order to address any queries, concerns, or technical issues the Customer may encounter or experience while using the Service.

9 Exclusions

The above service availability service level shall not apply to any unavailability, suspension or termination of the Service:

9.1 caused by a Force Majeure Event;

9.2 that results from any actions or omissions of the Customer in breach of the Contract;

9.3 that results from the Customer's equipment, software or other technology and/or third-party equipment, software or other technology;

9.4 that results from scheduled downtime and/or maintenance (planned or emergency);

9.5 related to any other service provided by Onecom (whether or not distinct service levels may apply to such service); or

9.6 arising from Onecom's suspension and/or termination of the Service in accordance with the Contract.

10 Planned and emergency maintenance

10.1 Planned outages may be required for scheduled maintenance and upgrade activities. Onecom will use reasonable endeavours, where possible, to effect such maintenance during Planned Maintenance Hours and give the Customer advance notice of any planned maintenance.

10.2 It may be necessary, from time to time, to carry out emergency maintenance to the Service to maintain appropriate levels of service quality. Onecom will use reasonable endeavours to inform the Customer of the likely disruption period at the earliest opportunity and, where necessary, work with Onecom's carrier partners to discourage maintenance without notification.

10.3 Emergency maintenance shall, wherever possible, take place during Planned Maintenance Hours and be notified to the Customer as soon as practical. The Customer acknowledges that it may not be possible to provide the Customer with advance notification of emergency maintenance.