# End User Licence Agreement

IMPORTANT NOTICE: PLEASE READ CAREFULLY BEFORE PROCEEDING. This end user licence agreement (EULA) is a legal agreement between you (Customer or you) and CybSafe Ltd (CybSafe) incorporated and registered in England and Wales with company number 9642350 whose registered office is at 5 New St Square, London EC4A 3TW for the use of the subscription services provided by CybSafe via an authorised reseller to you under this EULA via **https://cybsafe.com**.

**AGREED TERMS**

1. **INTERPRETATION**

**1.1.** The definitions and rules of interpretation in this clause apply in this EULA.

**1.1.1. Agreed Terms:** The agreement made between the Customer and the Authorised Reseller for the provision of the Services.

**1.1.2. Analytical Data:** the data provided to the Customer via the Services and in accordance with the Documentation detailing the Authorised Users use of the Services.

**1.1.3. Authorised Reseller:** a person authorised by CybSafe to resell and distribute the Services

**1.1.4. Authorised Users:** those employees, agents and independent contractors of the Customer who are authorised by the Customer to use the Services and the Documentation, as further described in clause 2.2(d).

**1.1.5. Business Day:** a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business.

**1.1.6. Complaint:** a complaint or request relating to either party's obligations under Data Protection Laws relevant to this Agreement, including any compensation claim from a Data Subject or any notice, investigation or other action from a Supervisory Authority;

**1.1.7. Confidential Information:** information that is proprietary or confidential and is either clearly labelled as such or identified as Confidential Information in clause 7.6.

**1.1.8. Core Hours:** 6.00am to 9.00pm local UK time, each Business Day.

**1.1.9. Customer Code:** the unique reference number or link specified by CybSafe and provided to the Customer by the Authorised Reseller which allows a Customer to access the Service.

**1.1.10. Customer Data:** the data inputted by the Customer, Authorised Users, or an Authorised Reseller on the Customer's behalf for the purpose of using the Services or facilitating the Customer's use of the Services.

**1.1.11. Data Controller**: has the meaning set out in the Data Protection Laws;

**1.1.12. Data Processor**: has the meaning given to that term (or to the term 'processor') in the Data Protection Laws;

**1.1.13. Data Protection Laws**:

(i) the Data Protection Act 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426 and/or

(ii) the General Data Protection Regulation (UK GDPR), once applicable, and/or any corresponding or equivalent United Kingdom national laws or regulations (Revised UK DP Law);

(iii) and, in either case any judicial or administrative interpretation of any of the above, any guidance, guidelines, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant Supervisory Authority

**1.1.14. Data Subject**: has the meaning set out in the Data Protection Laws;

1.1.15. **Data Subject Request**: a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws;

1.1.16. **Documentation:** the document made available to the Customer by CybSafe online via **https://cybsafe.com** or such other web address notified by CybSafe to the Customer from time to time which sets out a description of the Services and the user instructions for the Services.

1.1.17. **Normal Business Hours:** 8.00am to 6.00pm local UK time, each Business Day.

1.1.18. **Personal Data**: has the meaning given to that term in the Data Protection Laws and relates only to personal data, or any part of such personal data, in respect of which the both parties are Independent Data Controllers and in relation to which Cybsafe is providing services under this Agreement

1.1.19. **Services:** the subscription services provided by CybSafe to the Customer under this EULA via **https://cybsafe.com** or any other website notified to the Customer by CybSafe from time to time, as more particularly described in the Documentation.

1.1.20. **Software:** the online software applications provided by CybSafe as part of the Services.

1.1.21. **Subscription Term:** The Subscription Term agreed between the Customer and an Authorised Reseller

1.1.22. **Supervisory Authority**: any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws

1.1.23. **User Subscriptions:** the user subscriptions purchased by the Customer from an Authorised Reseller which entitle Authorised Users to access and use the Services and the Documentation in accordance with this EULA.

1.1.24. **Virus:** any thing or device (including any software, code, file or programme) which may: prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network, any telecommunications service, equipment or network or any other service or device; prevent, impair or otherwise adversely affect access to or the operation of any programme or data, including the reliability of any programme or data (whether by re-arranging, altering or erasing the programme or data in whole or part or otherwise); or adversely affect the user experience, including worms, trojan horses, viruses and other similar things or devices.

1.2. Clause, schedule and paragraph headings shall not affect the interpretation of this EULA.

1.3. A person includes an individual, corporate or unincorporated body (whether or not having separate legal personality) and that person's legal and personal representatives, successors or permitted assigns.

1.4. A reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established.

1.5. Unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular.

1.6. Unless the context otherwise requires, a reference to one gender shall include a reference to the other genders.

1.7. A reference to a statute or statutory provision is a reference to it as it is in force as at the date of this EULA.

1.8. A reference to a statute or statutory provision shall include all subordinate legislation made as at the date of this EULA under that statute or statutory provision.

1.9. A reference to writing or written includes faxes but not e-mail.

1.10. References to clauses and schedules are to the clauses and schedules of this EULA; references to paragraphs are to paragraphs of the relevant schedule to this EULA.

1.11. A reference to a **holding company** or a **subsidiary** means a holding company or a subsidiary (as the case may be) as defined in section 1159 of the Companies Act 2006. In the case of a limited liability partnership

which is a subsidiary of a company or another limited liability partnership, section 1159 of the Companies Act 2006 shall be construed so that: (a) references in sections 1159(1)(a) and (c) to voting rights are to the members' rights to vote on all or substantially all matters which are decided by a vote of the members of the limited liability partnership; and (b) the reference in section 1159(1)(b) to the right to appoint or remove a majority of its board of directors is to the right to appoint or remove members holding a majority of the voting rights.

## 2. SERVICES

**2.1.** Subject to the restrictions set out in this clause 2 and the other terms and conditions of this EULA, CybSafe hereby grants to the Customer a non-exclusive, non-transferable right to permit the Authorised Users to use the Services and the Documentation during the Subscription Term solely for the Customer's internal business operations.

**2.2.** In relation to the Authorised Users, the Customer undertakes that:

**2.2.1.** the maximum number of Authorised Users that it authorises to access and use the Services and the Documentation shall not exceed the number of User Subscriptions it has purchased from time to time;

**2.2.2.** it will not allow or suffer any User Subscription to be used by more than one individual Authorised User;

**2.2.3.** each Authorised User shall keep a secure password for his use of the Services and Documentation, and that each Authorised User shall keep his password confidential;

**2.2.4.** it shall maintain a written, up to date list of current Authorised Users and provide such list to CybSafe or the Authorised Reseller through whom it purchases the Services within 5 Business Days of CybSafe's written request at any time or times;

**2.2.5.** it shall permit CybSafe to audit the Services in order to establish the name and password of each Authorised User. Such audit may be conducted no more than once per quarter, at CybSafe's expense, and this right shall be exercised with reasonable prior notice, in such a manner as not to substantially interfere with the Customer's normal conduct of business; and

**2.2.6.** if any of the audits referred to in clause 2.2(e) reveal that any password has been provided to any individual who is not an Authorised User, then without prejudice to CybSafe's other rights, the Customer shall promptly disable such passwords and CybSafe shall not issue any new passwords to any such individual.

**2.3.** The Customer shall not:

**2.3.1.** except as may be allowed by any applicable law which is incapable of exclusion by agreement between the parties:

**2.3.1.1.** and except to the extent expressly permitted under this EULA, attempt to copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the Software and/or Documentation (as applicable) in any form or media or by any means; or

**2.3.1.2.** attempt to reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the Software; or

**2.3.2.** access all or any part of the Services and Documentation in order to build a product or service which competes with the Services and/or the Documentation; or

**2.3.3.** use the Services and/or Documentation to provide services to third parties; or

**2.3.4.** subject to clause 13.1, license, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the Services and/or Documentation available to any third party except the Authorised Users, or

**2.3.5.** attempt to obtain, or assist third parties in obtaining, access to the Services and/or Documentation, other than as provided under this clause 2 and

**2.4.** The Customer shall use all reasonable endeavours to prevent any unauthorised access to, or use of, the Services and/or the Documentation and, in the event of any such unauthorised access or use, promptly notify the Authorised Reseller.

**2.5.** The rights provided under this clause 2are granted to the Customer only, and shall not be considered granted to any subsidiary or holding company of the Customer unless the Authorised Reseller agrees otherwise in writing.

**2.6.** CybSafe shall, during the Subscription Term, provide the Services and make available the Documentation to the Customer on and subject to the terms of this EULA.

## 3. CUSTOMER DATA

**3.1.** The Customer shall own all right, title and interest in and to all of the Customer Data and shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of the Customer Data.

**3.2.** CybSafe shall follow its archiving procedures for Customer Data and the Analytical Data as set out in its Back-Up Policy available at **https://cybsafe.com** or such other website address as may be notified to the Customer from time to time, as such document may be amended by CybSafe in its sole discretion from time to time. In the event of any loss or damage to Customer Data or Analytical Data, the Customer's sole and exclusive remedy shall be for CybSafe to use reasonable commercial endeavours to restore the lost or damaged Customer Data or Analytical Data from the latest back-up of such Customer Data or Analytical Data maintained by CybSafe in accordance with the archiving procedure described in its Back-Up Policy. CybSafe shall not be responsible for any loss, destruction, alteration or disclosure of Customer Data caused by any third party (except those third parties sub-contracted by CybSafe to perform services related to Customer Data maintenance and back-up).

## 4. DATA PROTECTION

**4.1.** With respect to the rights and obligations under this written arrangement, the Customer and CybSafe acknowledge that they act as independent controllers and process Personal Data as set out in schedule 2 to perform their obligations governed by this Agreement in respect of their respective roles.

**4.2.** The Parties shall comply at all times with and assist each other in complying with their respective responsibilities for compliance with the obligations of Privacy and Data Protection Requirements in connection with the processing of Personal Data only as set out in Schedule 2 as updated in writing between the Parties from time to time, unless required to process the Personal Data for any other purpose by applicable Law in which case, where legally permitted, Customer or Cybsafe must inform the other of this legal requirement before processing.

**4.3.** Each Party agrees to their respective responsibilities and duties regarding processing as set out in Schedule 2 including to:

**4.3.1.** comply with data protection by design and data protection by default obligations under Privacy and Data Protection Requirements, including, where required, legitimate interest assessments and data protection impact assessments and associated consultation with data subjects, other Parties involved with the processing and any applicable supervisory authority, to ensure appropriate technical and organisational measures, including appropriate data protection governance and audit compliance, are implemented to safeguard the rights and freedoms of data subjects;

**4.3.2.** observe the principles of Privacy and Data Protection Requirements, including not retaining any of Personal Data for longer than is necessary to perform its obligations under this Agreement and upon the other Party's reasonable request, securely destroy (unless applicable Laws require continued storage of Personal Data) or return such Personal Data;

**4.3.3.** only transfer any Personal Data outside of theUnited Kingdom (the "UK") relying on Adequacy Decisions by the Commissioner or on appropriate standard contractual clauses ("Model Clauses") between the Parties. In the event that the Adequacy Decision granted in respect of the Model Clauses is invalidated or suspended, or any supervisory authority requires transfers of personal information pursuant to such Model Clauses to be suspended, then the Parties may require to:

4.3.3.1. cease data transfers forthwith, and implement an alternative adequacy mechanism (as agreed in writing by the Parties); or

4.3.3.2. return all Personal Data previously transferred and ensure that a senior officer or director of the Customer or Supplier certifies to the other that this has been done.

4.4. Monitor for, investigate and manage any actual or suspected personal data breach regarding processing activities undertaken by them, to inform the other Party of such personal data breaches without undue delay, and the other Party's sole and exclusive remedy shall be for the first Party to use reasonable commercial endeavours to resolve the personal data breach;

4.5. Comply with and provide information notices to data subjects regarding processing activities undertaken by them, including personal data breaches – such notices being available at https://www.cybsafe.com/website-privacy-policy/ such other website address as may be notified to the other Party from time to time, as such document may be amended from time to time by the first Party in its sole discretion;

4.6. Notify any applicable law enforcement authority (including any applicable supervisory authority) regarding personal data breaches where required relating to processing activities undertaken by them;

4.7. Fulfil any data subject rights request pertaining to their Personal Data or assist the other Party in doing so – such requests to be passed to the other Party within two working days in order to fulfil that request;

4.8. Notify the other Party without undue delay in writing if it receives from any applicable law enforcement authorities (including any applicable regulators) where permitted to do so:

4.8.1. any communication seeking to exercise rights conferred on the data subject by Privacy and Data Protection Requirements;

4.8.2. any complaint or any claim for compensation arising from or relating to the processing of Personal Data as set out in Schedule 2

4.8.3. any communication from any applicable law enforcement authorities (including any applicable regulators);

4.9. Provide such information and such assistance to the other Party as they may reasonably require, and within the timescales reasonably specified by the Parties, to allow the other Party to comply with their data protection by design and data protection by default obligations under Privacy and Data Protection Requirements, including, where required, consultation regarding legitimate interest assessments and data protection impact assessments, to ensure appropriate technical and organisational measures, including appropriate data protection governance and audit compliance, are implemented to safeguard the rights and freedoms of data subjects, including such full and prompt information and assistance to the other Party and any applicable law enforcement authorities (including any applicable regulators) in relation to a personal data breach.

4.10. Each Party shall designate a contact point for data subjects.

4.11. The Parties agree that they shall at no additional cost, keep or cause to be kept such information as is necessary to demonstrate compliance with their respective obligations under this clause (Data Protection) regarding the joint processing of Personal Data as set out in Schedule 2 carried out by the Parties in writing and in electronic form, and shall, upon reasonable notice, make available to the other Party or grant to the other Party and its auditors and agents, and any applicable law enforcement authority (including any applicable supervisory authority), a right of access to, and to take copies of, any information or records kept by the other Party pursuant to this clause (Data Protection) – this information to contain no less than:

4.11.1. their name and contact details, including those of its Companies, and, where applicable, of their representative, and their data protection officer;

4.11.2. the details regarding their respective processing set out in schedule 2

4.11.3. a general description of the appropriate technical and organisational measures to protect Personal Data against accidental or unlawful processing, loss, destruction, damage, alteration, or unauthorised disclosure or access, including so as to allow the Parties to comply with their obligations under Privacy and Data Protection Requirements – in particular:

4.11.3.1. to safeguard against the specific offences:

4.11.3.2. for a person knowingly or recklessly to re-identify Personal Data that is de-identified Personal Data without the consent of the controller responsible for de-identifying the personal data.

**4.11.3.3.** to alter, deface, block, erase, destroy or conceal Personal Data with the intention of preventing disclosure of all or part of the Personal Data that the person making the request would have been entitled to receive.

**4.11.4.** where transferring Personal Data to a third country or an international organisation, the identification of that third country or international organisation and, in the case of ex-UK transfers without adequacy, binding corporate rules, code of conduct, data protection seals, or standard contractual clauses, the documentation of appropriate safeguards such as:

**4.11.4.1.** explicit consent from affected data subjects, or

**4.11.4.2.** evidence that the transfer is required for the performance or conclusion of the performance of a contract with said data subjects.

**4.11.5.** ensure that any staff or personnel (including contractors) authorised to process Personal Data shall be subject to a binding duty of confidentiality in respect of such data.

**4.12.** The Parties agree to notify each other immediately if, in the opinion of the other Party, the written arrangement for the processing of Personal Data given by the Customer or CybSafe violates any provision of Privacy and Data Protection Laws

**4.13.** Neither Party shall perform their obligations under this Agreement in such a way as to cause the other Party to violate any of their respective obligations under Privacy Data Protection Requirements..

**4.14.** Whereas neither Party shall be responsible for accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, by the other Party, both Parties shall be liable where the data subject may exercise his or her rights under Privacy and Data Protection Requirements..

**4.15.** For the purposes of this clause (Data Protection), "controller", "joint controller", "processor", "data subject", "personal data", "processing", "personal data breach" and "appropriate technical and organisational measures" will be interpreted in accordance with Privacy and Data Protection Requirements..

**4.16.** The parties agree that on the date of this Agreement they shall complete all relevant details in, and enter into, Schedule 2 in particular the role of each Party, the subject-matter, nature, scope, context (including duration of the processing) and purpose of the processing, the type of personal data and categories of data subjects.

## 5. CYBSAFE'S OBLIGATIONS

**5.1.** CybSafe undertakes that the Services will be performed substantially in accordance with the Documentation and with reasonable skill and care.

**5.2.** The undertaking at clause 5.1 shall not apply to the extent of any non-conformance which is caused by use of the Services contrary to CybSafe's instructions, or modification or alteration of the Services by any party other than CybSafe or CybSafe's duly authorised contractors or agents. If the Services do not conform with the foregoing undertaking, CybSafe will, at its expense, use all reasonable commercial endeavours to correct any such non-conformance promptly, or provide the Customer with an alternative means of accomplishing the desired performance. Such correction or substitution constitutes the Customer's sole and exclusive remedy for any breach of the undertaking set out in clause 5.1. Notwithstanding the foregoing, CybSafe:

**5.2.1.** does not warrant that the Customer's use of the Services will be uninterrupted or error-free; or that the Services, Documentation and/or the information obtained by the Customer through the Services will meet the Customer's requirements; and

**5.2.2.** is not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the internet, and the Customer acknowledges that the Services and Documentation may be subject to limitations, delays and other problems inherent in the use of such communications facilities.

## 6. CUSTOMER'S OBLIGATIONS

**6.1.** The Customer shall:

**6.1.1.** comply with all applicable laws and regulations with respect to its activities under this EULA;

**6.1.2.** ensure that the Authorised Users use the Services and the Documentation in accordance with the terms and conditions of this EULA and shall be responsible for any Authorised User's breach of this EULA;

**6.1.3.** obtain and shall maintain all necessary licences, consents, and permissions necessary for CybSafe, its contractors and agents to perform their obligations under this EULA, including without limitation the Services;

**6.1.4.** ensure that its network and systems comply with the relevant specifications provided by CybSafe from time to time; and

**6.1.5.** be solely responsible for procuring and maintaining its network connections and telecommunications links from its systems to CybSafe's data centres, and all problems, conditions, delays, delivery failures and all other loss or damage arising from or relating to the Customer's network connections or telecommunications links or caused by the internet.

## 7. PROPRIETARY RIGHTS

**7.1.** The Customer acknowledges and agrees that CybSafe and/or its licensors own all intellectual property rights in the Services and the Documentation. Except as expressly stated herein, this EULA does not grant the Customer any rights to, or in, patents, copyright, database right, trade secrets, trade names, trade marks (whether registered or unregistered), or any other rights or licences in respect of the Services or the Documentation.

**7.2.** CybSafe confirms that it has all the rights in relation to the Services and the Documentation that are necessary to grant all the rights it purports to grant under, and in accordance with, the terms of this EULA.

## 8. CONFIDENTIALITY

**8.1.** Each party may be given access to Confidential Information from the other party in order to perform its obligations under this EULA. A party's Confidential Information shall not be deemed to include information that:

**8.1.1.** is or becomes publicly known other than through any act or omission of the receiving party;

**8.1.2.** was in the other party's lawful possession before the disclosure;

**8.1.3.** is lawfully disclosed to the receiving party by a third party without restriction on disclosure; or

**8.1.4.** is independently developed by the receiving party, which independent development can be shown by written evidence;

**8.2.** Each party shall hold the other's Confidential Information in confidence and, unless required by law or as permitted by clause 8.3, not make the other's Confidential Information available to any third party, or use the other's Confidential Information for any purpose other than the implementation of this EULA. To the extent that a party is compelled to disclose Confidential Information to any court or competent jurisdiction or by any regulatory or administrative body, such party shall, where permitted by applicable law, notify the other party in writing of such compelled disclosure prior to (or if not possible, as soon as reasonably practicable after) disclosing any Confidential Information to such third party provided always that the relevant party shall limit the disclosure of Confidential Information to the extent necessary to comply with applicable law.

**8.3.** CybSafe shall be permitted to share the following limited information with the Authorised Reseller from whom the Customer purchased the Services: Customer name, account status (active/inactive); number of Authorised Users; overview performance statistics; expiry date of current subscription term.

**8.4.** Each party shall take all reasonable steps to ensure that the other's Confidential Information to which it has access is not disclosed or distributed by its employees or agents in violation of the terms of this EULA.

**8.5.** Neither party shall be responsible for any loss, destruction, alteration or disclosure of Confidential Information caused by any third party.

**8.6.** The Customer acknowledges that details of the Services, and the results of any performance tests of the Services, constitute CybSafe's Confidential Information.

**8.7.** CybSafe acknowledges that the Customer Data is the Confidential Information of the Customer.

**8.8.** This clause 7 shall survive termination of this EULA, however arising.

**8.9.** No party shall make, or permit any person to make, any public announcement concerning this EULA without the prior written consent of the other parties (such consent not to be unreasonably withheld or delayed), except as required by law, any governmental or regulatory authority (including, without limitation, any relevant securities exchange), any court or other authority of competent jurisdiction.

## 9. INDEMNITY

**9.1.** CybSafe shall defend the Customer, its officers, directors and employees against any claim that the Services or Documentation infringes any United Kingdom patent effective as of the date that the Customer first accesses the Services, copyright, trade mark, database right or right of confidentiality, and shall indemnify the Customer for any amounts awarded against the Customer in judgment or settlement of such claims, provided that:

**9.1.1.** CybSafe is given prompt notice of any such claim;

**9.1.2.** the Customer provides reasonable co-operation to CybSafe in the defence and settlement of such claim, at CybSafe's expense; and

**9.1.3.** CybSafe is given sole authority to defend or settle the claim.

**9.2.** In the defence or settlement of any claim, CybSafe may procure the right for the Customer to continue using the Services, replace or modify the Services so that they become non-infringing or, if such remedies are not reasonably available, terminate this EULA on 2 Business Days' notice to the Customer without any additional liability or obligation to pay liquidated damages or other additional costs to the Customer.

**9.3.** In no event shall CybSafe, its employees, agents and sub-contractors be liable to the Customer to the extent that the alleged infringement is based on:

**9.3.1.** a modification of the Services or Documentation by anyone other than CybSafe; or

**9.3.2.** the Customer's use of the Services or Documentation in a manner contrary to the instructions given to the Customer by CybSafe; or

**9.3.3.** the Customer's use of the Services or Documentation after notice of the alleged or actual infringement from CybSafe or any appropriate authority.

**9.4.** The foregoing states the Customer's sole and exclusive rights and remedies, and CybSafe's (including CybSafe's employees', agents' and sub-contractors') entire obligations and liability, for infringement of any patent, copyright, trade mark, database right or right of confidentiality.

## 10. LIMITATION OF LIABILITY

**10.1.** This clause 9 sets out the entire financial liability of CybSafe (including any liability for the acts or omissions of its employees, agents and sub-contractors) to the Customer:

**10.1.1.** arising under or in connection with this EULA;

**10.1.2.** in respect of any use made by the Customer of the Services and Documentation or any part of them; and

**10.1.3.** in respect of any representation, statement or tortious act or omission (including negligence) arising under or in connection with this EULA.

**10.2.** Except as expressly and specifically provided in this EULA:

**10.2.1.** the Customer assumes sole responsibility for results obtained from the use of the Services and the Documentation by the Customer, and for conclusions drawn from such use;

**10.2.2.** all warranties, representations, conditions and all other terms of any kind whatsoever implied by statute or common law are, to the fullest extent permitted by applicable law, excluded from this EULA; and

**10.2.3.** the Services and the Documentation are provided to the Customer on an "as is" basis.

**10.3.** Nothing in this EULA excludes the liability of CybSafe:

**10.3.1.** for death or personal injury caused by CybSafe's negligence; or

**10.3.2.** for fraud or fraudulent misrepresentation.

**10.4.** Subject to clause 9.2 and clause 9.3:

**10.4.1.** CybSafe shall not be liable whether in tort (including for negligence or breach of statutory duty), contract, misrepresentation, restitution or otherwise for any loss of profits, loss of business, depletion of goodwill and/or similar losses or loss or corruption of data or information, or pure economic loss, or for any special, indirect or consequential loss, costs, damages, charges or expenses however arising under this EULA; and

**10.4.2.** CybSafe's total aggregate liability in contract tort (including negligence or breach of statutory duty), misrepresentation, restitution or otherwise, arising in connection with the performance or contemplated performance of this EULA shall be limited to the total subscription fees paid by the Authorised Reseller to CybSafe for the User Subscriptions during the 12 months immediately preceding the date on which the claim arose.

## 11. TERM AND TERMINATION

**11.1.** This EULA shall, unless otherwise terminated as provided in this clause 10, commence on the date agreed between the Customer and the Authorised Reseller and will terminate when the Agreed Terms terminate or expire.

**11.2.** Without affecting any other right or remedy available to it, either party may terminate this EULA with immediate effect by giving written notice to the other party if:

**11.2.1.** the other party fails to pay any amount due under this EULA on the due date for payment and remains in default not less than 20 days after being notified in writing to make such payment;

**11.2.2.** the other party commits a material breach of any other term of this EULA which breach is irremediable or (if such breach is remediable) fails to remedy that breach within a period of 30 days after being notified in writing to do so;

**11.2.3.** the other party commences negotiations with all or any class of its creditors with a view to rescheduling any of its debts, or makes a proposal for or enters into any compromise or arrangement with its creditors other than for the sole purpose of a scheme for a solvent amalgamation of that other party with one or more other companies or the solvent reconstruction of that other party;

**11.2.4.** a petition is filed, a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up of that other party other than for the sole purpose of a scheme for a solvent amalgamation of that other party with one or more other companies or the solvent reconstruction of that other party;

**11.2.5.** an application is made to court, or an order is made, for the appointment of an administrator, or if a notice of intention to appoint an administrator is given or if an administrator is appointed, over the other party;

**11.2.6.** the holder of a qualifying floating charge over the assets of that other party has become entitled to appoint or has appointed an administrative receiver;

**11.2.7.** a person becomes entitled to appoint a receiver over the assets of the other party or a receiver is appointed over the assets of the other party;

**11.2.8.** a creditor or encumbrancer of the other party attaches or takes possession of, or a distress, execution, sequestration or other such process is levied or enforced on or sued against, the whole or any part of the other party's assets and such attachment or process is not discharged within 14 days;

**11.2.9.** any event occurs, or proceeding is taken, with respect to the other party in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned in clause 10.2(c) to clause 10.2(h) (inclusive).

**11.3.** On termination of this EULA for any reason:

**11.3.1.** all licences granted under this EULA shall immediately terminate;

**11.3.2.** CybSafe may terminate any licence granted to Authorised Users in connection with the use of a mobile application as part of the Services;

**11.3.3.** each party shall return and make no further use of any equipment, property, Documentation and other items (and all copies of them) belonging to the other party;

**11.3.4.** CybSafe may destroy or otherwise dispose of any of the Customer Data and the Analytical Data in its possession unless CybSafe receives, no later than ten days after the effective date of the termination of this EULA, a written request for the delivery to the Customer of the then most recent back-up of the Customer Data and Analytical Data. CybSafe shall use reasonable commercial endeavours to deliver the back-up to the Customer within 30 days of its receipt of such a written request, provided that the Customer has, at that time, paid all fees and charges outstanding at and resulting from termination (whether or not due at the date of termination). The Customer shall pay all reasonable expenses incurred by CybSafe in returning or disposing of Customer Data and Analytical Data or providing the Customer with a back-up copy of such data; and

**11.3.5.** any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination, including the right to claim damages in respect of any breach of the agreement which existed at or before the date of termination shall not be affected or prejudiced.

## 12. FORCE MAJEURE

CybSafe shall have no liability to the Customer under this EULA if it is prevented from or delayed in performing its obligations under this EULA, or from carrying on its business, by acts, events, omissions or accidents beyond its reasonable control, including, without limitation, strikes, lock-outs or other industrial disputes (whether involving the workforce of CybSafe or any other party), failure of a utility service or transport or telecommunications network, act of God, war, riot, civil commotion, malicious damage, compliance with any law or governmental order, rule, regulation or direction, accident, breakdown of plant or machinery, fire, flood, storm or default of suppliers or sub-contractors, provided that the Customer is notified of such an event and its expected duration.

## 13. GENERAL

**13.1. Conflict.** If there is an inconsistency between any of the provisions in the Agreed Terms, the main body of this EULA and the Schedule, the provisions shall take precedence in the order stated in this clause 15.1.

**13.2. Variation.** CybSafe shall be entitled to vary the terms of this EULA by giving the Customer 30 days notice by email. No other variation of this EULA shall be effective unless it is in writing and signed by the parties (or their authorised representatives). The administrator of the Customer's account shall be deemed to be an authorised representative of the Customer.

**13.3. Waiver.** No failure or delay by a party to exercise any right or remedy provided under this EULA or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

**13.4. Rights and Remedies.** Except as expressly provided in this EULA, the rights and remedies provided under this EULA are in addition to, and not exclusive of, any rights or remedies provided by law.

**13.5. Severance.** If any provision (or part of a provision) of this EULA is found by any court or administrative body of competent jurisdiction to be invalid, unenforceable or illegal, the other provisions shall remain in force.

**13.6.** If any invalid, unenforceable or illegal provision would be valid, enforceable or legal if some part of it were deleted, the provision shall apply with whatever modification is necessary to give effect to the commercial intention of the parties.

**13.7.** **Entire Agreement.** This EULA, and any documents referred to in it, constitute the whole agreement between the parties and supersede any previous arrangement, understanding or agreement between them relating to the subject matter they cover.

**13.8.** Each of the parties acknowledges and agrees that in entering into this EULA it does not rely on any undertaking, promise, assurance, statement, representation, warranty or understanding (whether in writing or not) of any person (whether party to this EULA or not) relating to the subject matter of this EULA, other than as expressly set out in this EULA.

**13.9.** **No Partnership or Agency.** Nothing in this EULA is intended to or shall operate to create a partnership between the parties, or authorise either party to act as agent for the other, and neither party shall have the authority to act in the name or on behalf of or otherwise to bind the other in any way (including, but not limited to, the making of any representation or warranty, the assumption of any obligation or liability and the exercise of any right or power).

**13.10.** **Third Party Rights.** This EULA does not confer any rights on any person or party (other than the parties to this EULA and, where applicable, their successors and permitted assigns) pursuant to the Contracts (Rights of Third Parties) Act 1999.

**13.11.** Sanctions. Each Party shall comply with all applicable economic sanctions laws and regulations, in the performance of this Agreement, including the use and transfer of any Products or Services subject to this Agreement.

**13.12.** Anti-Corruption. In relation to resale activities under this Agreement, each Party agrees:

It will comply with all applicable laws, ordinances and regulations of any jurisdiction, including the U.S. Foreign Corrupt Practices Act, the UK Bribery Act, and all other applicable anti-corruption, anti-money laundering laws, and competition laws (collectively "the Anti Corruption Laws). Neither Party will take any action, nor fail to take any action, that would result in the other Party violating any Anti Corruption Laws.

Neither Party will offer or give money or anything of value to any person, in order to obtain or retain business for the benefit of itself or the other Party, or to secure any other improper advantage for itself or the other Party. Any provision of gifts, meals, entertainment expenses or travel expenses must be (i) permissible under all applicable Anti Corruption Laws, and (ii) the recipient employer's internal policies.

It will not submit any false or inaccurate invoices or documentation to the other Party, and will submit true and adequate documentation with all invoices, including itemized expenses incurred, accompanied by receipts (or other documentation if a receipt is unavailable) identifying the payment date, amount and purpose of the expense. During the term of this Agreement and for three (3) years thereafter, for the purposes of inspecting compliance with the provisions of this Section 20, each Party (the "Non-Auditing Party") will retain and, upon reasonable notice, will provide the other Party (the "Auditing Party") reasonable access to audit the Non-Auditing Party's books, accounts, and records, including payments made by the Non-Auditing Party for or on behalf of the Auditing Party. At the Non-Auditing Party's option, the Auditing Party may select an independent third-party of international reputation and good standing to conduct the audit. The independent third-party will be required to agree to a non-disclosure agreement. The Non-Auditing Party shall cooperate fully in any audit conducted by or on behalf of the Auditing Party.

It will promptly notify the other Party (Non-breaching Party), in writing, if the breaching Party fails to comply with the provisions of this Agreement; If the Non-breaching Party has a good faith belief that there has been a breach of this provision, the Non-breaching Party may terminate its Agreement with the breaching Party immediately upon written notice and without penalty.

## 14. ASSIGNMENT

**14.1.** The Customer shall not, without the prior written consent of CybSafe (which shall not be unreasonable withheld or delayed), assign, transfer, charge, sub-contract or deal in any other manner with all or any of its rights or obligations under this EULA.

**14.2.** CybSafe may at any time assign, transfer, charge, sub-contract or deal in any other manner with all or any of its rights or obligations under this EULA.

15. **NOTICES**

**15.1.** Any notice required to be given under this EULA shall be in writing and shall be delivered by hand or sent by pre-paid first-class post or recorded delivery post or email to the other party at its address set out in this EULA, the customer portal at **https://cybsafe.com** or such other address as may have been notified by that party for such purposes.

**15.2.** A notice delivered by hand shall be deemed to have been received when delivered (or if delivery is not in business hours, at 9 am on the first business day following delivery). A correctly addressed notice sent by pre-paid first-class post or recorded delivery post shall be deemed to have been received at the time at which it would have been delivered in the normal course of post. A notice sent by email shall be deemed to have been received when sent.

16. **GOVERNING LAW AND JURISDICTION**

**16.1.** This EULA and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the law of England and Wales.

**16.2.** Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this EULA or its subject matter or formation (including non-contractual disputes or claims).

**THIS AGREEMENT** has been entered into on the date stated at the beginning of it.

**END OF MAIN DOCUMENT**

## SCHEDULE 1 – SERVICE LEVEL AGREEMENT

### 1. Interpretation

The following definitions and rules of interpretation apply in this schedule.

Definitions:

**Commercially Reasonable Efforts:** the same degree of priority and diligence with which Cybsafe meets the support needs of its other similar customers.

**Customer Cause:** any of the following causes:

**(a)** any improper use, misuse or unauthorised alteration of the Software or Services by the Customer;

**(b)** any use of the Software or Services by the Customer in a manner inconsistent with the then-current Documents; and

**(c)** outages or disruptions to the Service caused by the Customer.

**Fault:** any failure of the Services to operate in all material respects in accordance with the Documentation, including any failure or error referred to in the Service Level Table.

**Help Desk Support:** any support provided by help desk technicians sufficiently qualified and experienced to identify and resolve most support issues relating to the Services.

**Main Agreement:** the agreement to which this schedule relates.

**Out-of-scope Services:** any services provided by Cybsafe in connection with any apparent problem regarding the Services reasonably determined by Cybsafe not to have been caused by a Fault, but rather by a Customer Cause or a cause outside Cybsafe's control (including any investigational work resulting in such a determination).

**Service Levels:** the service levels set out in paragraph 5.1.

**Solution:** either of the following outcomes:

**(a)** correction of a Fault; or

**(b)** a workaround in relation to a Fault (including a reversal of any changes to the Software and/or Services if deemed appropriate by Cybsafe) that is reasonably acceptable to the Customer.

**Support Request:** request made by the Customer in accordance with this schedule for support in relation to the Services, including correction of a Fault.

**Support Services:** Maintenance of the Software and providing Help Desk Support but excluding any Out-of-scope Services.

All initial capitalised terms in this schedule shall have the meaning given to them in the Main Agreement.

### 2. Support Services

During the Subscription Term Cybsafe shall perform the Support Services during the Normal Business Hours in accordance with the Service Levels.

As part of the Support Services, Cybsafe shall:

**(a)** provide Help Desk Support by means of the following e-mail address helpdesk@cybsafe.com and by means of the help desk support page;

**(b)** use Commercially Reasonable Efforts to correct all Faults notified under paragraph (a); and

**(c)** provide technical support for the Software and the Services in accordance with the Service Levels.

Cybsafe shall carry out planned maintenance outside of the Core Hours; and

Cybsafe may reasonably determine that any services are Out-of-scope Services. If Cybsafe makes any such determination, it shall promptly notify the Customer of that determination.

The Customer acknowledges that Cybsafe is not obliged to provide Out-of-scope Services.

### 3. Fees

The provision of Support Services on a remote (via email), off-site basis within the Subscription Term shall be included in the fees you pay to our Authorised Reseller

The provision of Support Services outside the Subscription Term or at the Customer's premises or the provision of Out-of-scope Services shall be charged at the time and materials rates agreed between the parties when the Out-of-Scope Services are requested.

### 4. Submitting Support Requests and access

The Customer may request Support Services by way of a Support Request made via email by completing the support request form on the help desk support page.

Each Support Request shall include a description of the problem and the start time of the incident.

The Customer shall provide Cybsafe with:

**(a)** prompt notice of any Faults; and

**(b)** such output and other data, documents, information, assistance and (subject to compliance with all Customer's security and encryption requirements notified to Cybsafe in writing) remote access to the Customer System, as are reasonably necessary to assist Cybsafe to reproduce operating conditions similar to those present when the Customer detected the relevant Fault and to respond to the relevant Support Request.

All Support Services shall be provided remotely by Cybsafe.

### 5. Service Levels

**Service Availability and Maintenance.** Cybsafe shall use commercially reasonable endeavours to make the Services available 97% of the time during the Core Hours, except for unscheduled maintenance performed during the Core Hours, provided that Cybsafe has used reasonable endeavours to give the Customer at least 3 Business Hours' notice in advance.

**Support** Cybsafe shall:

**(a)** prioritise all Support Requests based on its reasonable assessment of the severity level of the problem reported; and

**(b)** respond to all Support Requests within the response times specified in the table set out below by acknowledging receipt of the Support Request and commencing Commercially Reasonable Efforts to achieve a Solution:

| Severity level of Fault | Definition | Service Level response time* |
|---|---|---|
| 1 | **Fatal:** An error in, or failure of, the Services such that the Services are unavailable to all Authorised Users | 4 Normal Business Hours |
| 2 | **Severe:** An error in, or failure of, the Services with more than 25% of Authorised Users or critical functions affected but which is not a Fatal Fault. Use of Services is intermittent. | 12 Normal Business Hours |
| 3 | **Medium:** An error in, or failure of, the Services:<br>a) that affects between more than 10% number of Authorised Users but which is not a Fatal or Severe Fault; and/or<br>b) that affects a limited number of functions;but the Services can still be used. | 24 Normal Business Hours |

| | | |
|---|---|---|
| 4 | **Minor:** An error in, or failure of, the Services that affects less than 10% of Authorised Users. The Service can still be used. | 3 Business Days |

*For the purposes of this table, where a Support Request is received outside Normal Business Hours, it shall be deemed to have been received upon the commencement of the next Normal Business Hour.

The parties may, on a case-by-case basis, agree in writing to a reasonable extension of the Service Level response times.

Cybsafe shall give the Customer regular updates of the nature and status of its efforts to correct any Fault.

All Support Requests shall be received and responded to in English

## 6. Escalation

If the Customer is not satisfied with the response or the response time, the Customer may escalate the Support Request to the parties' respective Relationship Managers.

## 7. Communications

In addition to the mechanisms for giving notice specified in clause 17 of the Main Agreement, the parties may communicate in respect of any matter referred to in this agreement by e-mail (unless specified otherwise).

**SCHEDULE 2 - DATA PROTECTION**

CybSafe provides an intelligent cyber security Awareness, Behaviour and Culture platform, for the Customer to actively manage human cyber risk by improving the online behaviours of personnel (the Service). The platform is delivered as a single online cloud-based Software as a Service (SaaS), which reveals and responds to reliable metrics and data-driven insights to actively manage human cyber risk and resilience. Ultimately, the platform allows the Customer to stop paying lip-service to the human side of the equation, meaningfully reduce human cyber risk, and use a tool that gets more efficient and effective over time – whilst providing the Customer with the data to prove it, thereby putting an end to the reliance on tick-box security awareness training and meaningless phishing simulation statistics. The standard components of the platform are:

Security Awareness Training

Intelligent Phishing Simulation

Risk Reduction Metrics

Insider Threat Risk Mitigation

Compliance & Risk: The Human Factor

Cyber Security Behaviour and Culture


**It is the role of the Customer to determine:**

The aims of using the Service to:

more effectively manage their cyber risk profile,

leverage ease of administration and reporting capabilities of the Service to streamline business processes including billing for the Service,

facilitate inclusive functions and features to improve the online behaviours of personnel, and

generate reports to enhance the Service, including the necessity to process personnel Personal Data with the intended effect on such personnel being to improve their performance and choices such that all Parties benefit through statistical information to make decisions;

That all the following personnel shall use the Service (users) to improve their online behaviours:

administrators in the HR department, that shall exclusively also have administration rights and access permissions to initiate all users and generate reports regarding their own and team members' performance,

managers from across the business, that shall also have access to People tab and generate reports regarding their own and team members' performance, and

members of staff, including contractors, that shall also have the ability to generate reports regarding their own performance; and

That the following features and functions of the Service shall be utilised:

Administration – administrators shall source the email addresses and contact details for all users to input on the platform to facilitate the configuration and use of, as well as rights and access permissions to, the Service by users,

Report generation – reports rely upon further inputs from users on the intuitive, easy-to-use platform, such inputs being systematically monitored and tracked using first and third party cookies and other similar technologies relating to the contact details, IP Addresses and responses of users. This may include special categories of Personal Data entered into free-text fields, utilising data analytics, artificial intelligence (AI) and machine learning techniques on an ongoing basis to - identify, match, combine and analyse such available inputs as well as derived profiles from AI-curated content, targeted learning, virtual cyber assistance, personalised 'nudge' interventions, simulated social engineering attacks, and practical assessments relating to the users to score their individual ratings regarding their current online performance and previous historic differentials. This is measured against a set of cyber risk criteria compiled in automatically generated reports to compare results individually and across all users that all scientifically address human cyber security risk on a single system. This is further underpinned by psychology and behavioural science, which supports users at the right time, in the right way, and in a way much more likely to influence behaviours and attitudes, and that makes it easy to track impact, progress, areas for improvement, and return on investment, such risk metrics, measurements, indicators, insights and advanced reporting being used for the following purposes:

profiling of users to quantify and demonstrably reduce the Customer's human cyber risk vis-a-vis their online behaviours, choices and performance are adequately understood and improving, as determined by the Customer, the retention period being determined by the Agreement and whilst the Customer administrator has authorised their access to the Service,

anonymised statistical output for billing, as determined by both Parties, the retention period to generate such bills from available usage being 7 years in case of handling enquiries and complaints, and

platform usage regarding security, load balancing and other performance management, as well as Service development and innovation, as determined by the Supplier, the retention period to generate such insight being 1 year,

And that such available inputs are in addition disclosed to and processed by other Parties, also joint controllers, within and outside the United Kingdom(UK) subject to the data protection provisions in this Agreement including, without limitation, the appropriate safeguards including adequacy, binding corporate rules, code of conduct, data protection seals, or standard contractual clauses.

**It is the role of the Supplier through the provision of the SaaS platform to determine:**

The aim of the Service in order to:

more effectively manage the cyber risk profile of the Customer by facilitating the functions and features to improve the online behaviours of Customer personnel,

leverage ease of administration and reporting capabilities of the Service to streamline business processes including billing for the Service, and

monitor and optimise the platform performance and security, including generating reports to enhance the Service,

Including the necessity to process personnel Personal Data with the intended effect on such personnel being to improve their performance and choices such that the all Parties benefit through statistical information to make decisions;

The means to most effectively provide rights and access permissions to the following:

administrators in the HR department, that shall exclusively also have administration rights and access permissions to initiate all users and generate reports regarding their own and team members' performance,

managers from across the business, that shall also have access to People tab and generate reports regarding their own and team members' performance, and

members of staff, including contractors, that shall also have the ability to generate reports regarding their own performance; and

The means to most effectively manage the processing of personnel Personal Data with regards to the following features and functions:

Administration – allowing administrators to input sourced email addresses and contact details for all users onto the platform and to facilitate the configuration and use of, as well as rights and access permissions to, the Service by users,

Report generation – reports rely upon further inputs from users on the intuitive, easy-to-use platform, such inputs being systematically monitored and tracked using first and third party cookies and other similar technologies relating to the contact details, IP Addresses and responses of users. This may include special categories of Personal Data entered into free-text fields, utilising data analytics, artificial intelligence (AI) and machine learning techniques on an ongoing basis to - identify, match, combine and analyse such available inputs as well as derived profiles from AI-curated content, targeted learning, virtual cyber assistance, personalised 'nudge' interventions, simulated social engineering attacks, and practical assessments relating to the users to score their individual ratings regarding their current online performance and previous historic differentials. This is measured against a set of cyber risk criteria compiled in automatically generated reports to compare results individually and across all users that all scientifically address human cyber security risk on a single system. This is further underpinned by psychology and behavioural science, which supports users at the right time, in the right way, and in a way much more likely to influence behaviours and attitudes, and that makes it easy to track impact, progress, areas for improvement, and return on investment, such risk metrics, measurements, indicators, insights and advanced reporting being used for the following purposes:

profiling of users to demonstrate that their online behaviours, choices and performance are adequately understood and improving, as determined by the Customer, the retention period being determined by the Agreement and whilst the Customer administrator has authorised their access to the Service, such Personal Data being secured deleted or returned as determined by the Agreement,

anonymised statistical output for billing, as determined by both Parties, the retention period to generate such bills from available usage being 7 years in case of handling enquiries and complaints, such Personal Data being secured deleted or returned as determined by the Agreement, and

platform usage regarding security, load balancing and other performance management, as well as Service development and innovation, as determined by the Supplier, the retention period to generate such insight being 1 year, such Personal Data being secured deleted or returned as determined by the Agreement,

And that such available inputs are in addition disclosed to and processed by other Parties, also joint controllers, within and outside the United Kingdom (UK) subject to appropriate safeguards including adequacy, binding corporate rules, code of conduct, data protection seals, or standard contractual clause

**END OF SCHEDULE**