SOFTWARE SUBSCRIPTION AGREEMENT TERMS AND CONDITIONS

PLEASE READ CAREFULLY BEFORE USING ANY SOFTWARE FROM CYBER RISK AWARE: This licence agreement ("**Licence**") is a legal agreement between you ("**Licensee**" or "**you**") and **CYBER RISK AWARE LIMITED** ("**Cyber Risk Aware**") incorporated and registered in Ireland with company number 575504 whose principal place of business is at Talent Garden Dublin, Claremont Avenue, Glasnevin, Dublin 11, Ireland; ("**Licensor, us**" or "**we**") for:

(i) the subscription services via www.cyberriskaware.com or any other website notified to you from time to time, as more particularly described in the Documentation (as defined below) (the "**Services**");

(ii) the security awareness communications materials (the "**Communications Materials**"); and

(iii) the printed materials and online or electronic documents made available from time to time which set out a description of the Services and user instructions for the Services, (the "**Documentation**").

We license use of the Software and the content to you on the basis of this Licence. We do not sell the Software or Content to you. We remain the owners of the Software and Content at all times.

BY AGREEING TO A DOCUMENT INCORPORATING THESE CYBER RISK AWARE LICENSE TERMS AND CONDITIONS ("THE TERMS") (AN "ORDERING DOCUMENT") CYBER RISK AWARE AND LICENSEE AGREE THAT THESE TERMS SHALL GOVERN THE RELATIONSHIP BETWEEN THE PARTIES AS TO ANY CYBER RISK AWARE PRODUCTS OR SERVICES PROVIDED OR TO BE PROVIDED TO LICENSEE AS SET FORTH IN SUCH ORDERING DOCUMENT. AS TO ANY PARTICULAR ORDERING DOCUMENT, THE ORDERING DOCUMENT, THE SERVICES DEFINITIONS AND SERVICE-SPECIFIC TERMS AND CONDITIONS, AND THESE TERMS TOGETHER CONSTITUTE THE AGREEMENT OF THE PARTIES AND ARE REFERRED TO COLLECTIVELY HEREIN AS THE "AGREEMENT." IN THE EVENT OF ANY CONFLICT BETWEEN THE ORDERING DOCUMENT AND THESE TERMS, THESE TERMS SHALL PREVAIL UNLESS THE ORDERING DOCUMENT EXPRESSLY PROVIDES THAT IT IS MODIFYING THESE TERMS WITH RESPECT TO SUCH AGREEMENT.

RECITALS:

Cyber Risk Aware has developed certain software applications and platforms which it makes available to subscribers via the Cyber Risk Aware platform to allow organisations monitor and test the readiness of their workforce and better protect themselves against phishing emails and SMS smishing text messages.

The Customer wishes to use Cyber Risk Aware's service in its business operations and make it available to its Users.

Cyber Risk Aware has agreed to provide, and the Customer has agreed to take and pay for Cyber Risk Aware's service, subject to the terms and conditions of this Agreement.

IT IS HEREBY AGREED:

1. INTERPRETATION

The definitions and rules of interpretation in this clause apply in this Agreement.

1.1. "**Affiliate**" means any entity which is directly or indirectly under the control of, controlled by, or under common control of a party, with control being defined as ownership of more than fifty percent (50%) of the voting shares or other controlling interest.

1.2. "**Agreement**" means this agreement and its exhibits.

1.3. "**Business Day**" means a day other than a Saturday, Sunday or public holiday in Ireland when banks in Dublin are open for business.

1.4. "**Communications Materials**" shall have the meaning ascribed to them in clause 3.1.

1.5. "**Confidential Information**" shall have the meaning ascribed to that term in clause 8.1.

1.6. "**Customer Content**" shall mean information and materials provided by the Customer or its Users or agents to Cyber Risk Aware, regardless of form, including, without limitation, its trademarks, trade names, service marks, logos and designs, e-mail addresses of personnel, and images, graphics, and text, in connection with the use of the Services.

1.7. "**Data Protection Legislation**" means all applicable data protection and privacy legislation in force from time to time in Ireland including the General Data Protection Regulation *(EU) 2016/679*); the Data Protection Acts 1988-2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (*SI 2003/2426*) as amended.

1.8. "**Disclosing Party**" shall have the meaning ascribed to that term in clause 8.1.

1.9. "**Documentation**" means the printed materials and online or electronic documents made available to the Customer by Cyber Risk Aware from time to time which set out a description of the Services and user instructions for the Services, including the Cyber Risk Aware Operational Procedures Manual set out from time in Exhibit B.

1.10. "**Exhibits**", means the exhibits to this Agreement and each an "**Exhibit**".

1.11. "**Fees**" means the Initial Subscription Fee and any Renewal Subscription Fee.

1.12. "**Hosted Software**" shall have the meaning ascribed to that term in clause 5.5.

1.13. "**Initial Subscription Fee**" shall have the meaning ascribed to in the ordering document.

1.14. "**Term**" shall have the meaning ascribed to that term in clause 7.2.

1.15. "**Intellectual Property Rights**" means patents, utility models, rights to inventions, copyright and related rights, trade marks and service marks, trade names and domain names, rights in get-up, goodwill and the right to sue for passing off or unfair competition, rights in designs, rights in computer software, database rights, rights to preserve the confidentiality of information (including know-how and trade secrets) and any other intellectual property rights, including all applications for (and rights to apply for and be granted), renewals or extensions of, and rights to claim priority from, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist, now or in the future, in any part of the world.

1.16. **"Licence"** has the meaning given to it in clause 2.1.

1.17. "**Material Breach**" shall be a misappropriation of a Party's Intellectual Property Rights.

1.18. "**Normal Business Hours**" means 8.00 am to 6.00 pm Irish time, each Business Day.

1.19. "**On-Site Software**" means the Software licensed and installed on a Customer or User PC, if applicable;

1.20. "**Receiving Party**" shall have the meaning ascribed to that term in clause 8.1.

1.21. "**Renewal Subscription Fee**" shall have the meaning ascribed to that term in clause 7.3.1.

1.22. "**Renewal Term**" shall have the meaning ascribed to that term in clause 7.2.

1.23. "**Services**" means the subscription services provided by Cyber Risk Aware to the Customer under this Agreement via www.cyberriskaware.com or any other website notified to the Customer from time to time, as more particularly described in the Documentation.

1.24. "**Software**" means PhishMaestro – Mock Phishing Platform, PhishHuk ("**PhishHuk Software**") (Outlook Plugin to report phishing emails), Staff CyberKnowledge Assessment Quiz, security awareness training modules, reporting, computer software, the data supplied with the software and the associated media, provided by Cyber Risk Aware as part of the Services.

1.25. "**Support Services**" shall mean the standard support services that Cyber Risk Aware will provide to the Customer and its Users as more particularly described at Exhibit C.

1.26. "**Suspect Email**" shall have the meaning ascribed to that term in clause 4.1.

1.27. "**Full Term**" means the Initial Term and any Renewal Term, unless terminated earlier in accordance with this Agreement.

1.28. "**User Subscriptions**" means the user subscriptions under the Licence purchased by the Customer pursuant to clause 6 which entitle the Customer and its Users to access and use the Services, the Communications Materials and the Documentation in accordance with this Agreement.

1.29. "**Users**" means the employees or other representatives, agents or contractors of the Customer who are authorized to use the Services, the Communication Materials and the Documentation.

1.30 "**Virus**" means 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.

1.31 "**Warranty Period**" shall have the meaning ascribed to that term in clause 11.

2. LICENCE AND USER SUBSCRIPTIONS

2.1. Subject to the Customer purchasing the User Subscriptions in accordance with clause 6 and clause 7.2 and the restrictions set out in clause 2 and the other terms and conditions of this Agreement, Cyber Risk Aware hereby grants to the Customer for the Term a non-exclusive, non-transferable right, without the right to grant sub-licences, to use and to permit its Users to access and use the Services, the Communications Materials and the Documentation during the Term solely for their internal business operations (the "**Licence**").

2.2. The Customer shall not, and the Customer shall procure that its Users shall not, access, store, distribute or transmit any Viruses, or any Customer Content or other material during the course of its use of the Services that:

a. is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive;

b. facilitates illegal activity;

c. depicts sexually explicit images;

d. promotes unlawful violence;

e. is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability; or

f. is otherwise illegal or causes damage or injury to any person or property;

and Cyber Risk Aware reserves the right, without liability or prejudice to its other rights to the Customer, to disable the Customer's (or any User's) access to any material that breaches the provisions of this clause.

2.3. The Customer shall not, and the Customer shall procure that its Users shall not:

a. except as may be allowed by any applicable law which is incapable of exclusion by agreement between the parties and except to the extent expressly permitted under this Agreement:

(i) attempt to copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the Software, Communications Materials and/or Documentation (as applicable) in any form or media or by any means; or

(ii) attempt to de-compile, reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the Software; or

b. 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

c. use the Services, the Communications Materials and/or Documentation to provide services to third parties, except the Users; or

d. subject to clause 14.5, licence, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the Services, the Communications Materials and/or Documentation available to any third party, or

e. attempt to obtain, or assist third parties in obtaining, access to the Services and/or Documentation, other than as provided under this clause 2.3.

2.3.1. The Customer shall use all reasonable endeavours to prevent any unauthorised access to, or use of, the Services, the Communications Materials and/or the Documentation and, in the event of any such unauthorised access or use, promptly notify Cyber Risk Aware.

2.3.2. The rights provided under this clause 2 are granted to the Customer only, and shall not be considered granted to any subsidiary or holding company of the Customer.

2.4. The Customer acknowledges and agrees that Cyber Risk Aware and/or its licensors own all Intellectual Property Rights in the Services (including the Software), the Communications Materials and the Documentation. Except as expressly stated herein, this Agreement does not grant the Customer, its Affiliates or Users any rights to, under or in, any 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, the Communications Materials or the Documentation.

2.5. Cyber Risk Aware confirms that it has all the rights in relation to the Services, the Communications Materials and the Documentation that are necessary to grant all the rights it purports to grant under, and in accordance with, the terms of this Agreement.

2.6. Cyber Risk Aware makes no claim of ownership to the Customer Content or to any Intellectual Property Rights in or to the Customer Content. All Intellectual Property Rights

owned by the Customer or its Users shall remain the property of the Customer and/or its Users.

3. SECURITY AWARENESS COMMUNICATIONS MATERIALS

3.1. Where Cyber Risk Aware licences Security Awareness Communications Materials (the "**Communications Materials**") to the Customer, it grants to the Customer a non-exclusive, non-transferable licence to the Communications Materials on the same terms as set out in clause 2 and the Customer acknowledges that additional restrictions on the use of the Communications Materials may be specified in Exhibit B.

3.2. The Communications Materials will be provided in digital download files only. Printing and other additional costs are the responsibility of Customer. Any attempt to sell, transfer, modify, copy, create derivative works from, broadcast or post on any external network or media the Communications Materials is prohibited.

3.3. Notwithstanding the foregoing, the Customer is permitted to broadcast or post the Communications Materials on or through the Customer's internal communications channels, including the Customer's internal network, internal computer systems or internal publications.

3.4. The Customer may in exercising its rights for the duration of this Agreement, brand the Communications Materials with the Customer's logo, with the Customer's own trademarks provided that Cyber Risk Aware takes no responsibility for such use, and the Customer will indemnify Cyber Risk Aware for any claims based on the Customer's use of trademarks on or in connection with the Communications Materials other than Cyber Risk Aware's trademarks.

4. PHISH MAESTRO

4.1. Where the Software licenced to the Customer includes PhishMaestro, the Customer acknowledges in licencing the Software, Cyber Risk Aware shall not have any responsibility to determine if any email received by the Customer or any User is a phishing attack (a "**Suspect Email**").

4.2. Cyber Risk Aware shall not be responsible for any damage to the Customer's network as a result of a Suspect Email and the Customer shall have the sole and exclusive obligation to evaluate any Suspect Email and take any and all actions the Customer determines are appropriate as a result of such Suspect Email.

5. SERVICES

5.1. Cyber Risk Aware shall, during the Term, provide the Services and make available the Documentation to the Customer and its Users on and subject to the terms of this Agreement.

5.2. Cyber Risk Aware shall use commercially reasonable endeavours to make the Services available 24 hours a day, seven days a week, except for:

5.2.1. planned maintenance carried out during the maintenance window of 10.00 pm to 2.00 am Irish time which will be communicated to the User in advance; and

5.2.2. unscheduled maintenance performed outside Normal Business Hours, provided that Cyber Risk Aware has used reasonable endeavours to give the Customer at least 6 Normal Business Hours' notice in advance.

5.3. Cyber Risk Aware will, as part of the Services and at no additional cost to the Customer provide the Customer with the Support Services. The Customer may purchase enhanced support services separately at Cyber Risk Aware's current rates.

5.4. In the performance of the Services:

5.4.1. Cyber Risk Aware will provide a dedicated User enrolment page which can be made available on the Customer portal and advertised as such. The User will input their relevant company details which Cyber Risk Aware require to automatically setup the User's portal. No manual enrollment will be required for each User.

5.4.2. If a User need assistance the User will raise a Cyber Risk Aware support call from within their portal "support request", by email or by telephone phone; and

5.4.3. the User administration dashboard will also be branded with the Customer logo.

5.5. The Software will be hosted on a served controlled by Cyber Risk Aware ("**Hosted Software**").

5.6. The Customer shall designate one or more valid domain names for the purpose of receiving fake phishing emails as part of the Services during the Term and such designated domain names may not be changed unless notified in writing to and agreed with Cyber Risk Aware.

6. CUSTOMER OBLIGATIONS

6.1. All Fees due hereunder are payable by the Customer in Euro.

6.2. If Cyber Risk Aware approves the Customer's request to purchase additional User Subscriptions, the Customer shall, within thirty (30) days of the date of Cyber Risk Aware's invoice, pay Cyber Risk Aware's list prices for such additional User Subscriptions.

6.3. Except to the extent set out in Exhibit A, the Initial Subscription Fee shall be payable in full on the Effective Date and this Initial Subscription Fee covers up to the number of Users set out in Exhibit A. Where the actual number of Users exceeds this amount at any time, additional fees shall be payable by the Customer according to Cyber Risk Aware's pricing model set out from time to time in Exhibit A. Such additional fees shall be payable within thirty (30) days of the date of invoice. New User Subscription requests, where approved will be activated by Cyber Risk Aware within three (3) days. The Renewal Subscription Fee shall be payable within thirty (30 days before the commencement of the respective Renewal Term.

6.4. Any taxes (except based on Cyber Risk Aware's income), duties, fees, or other charges levied by any government in connection with this Agreement shall be the responsibility of, and paid for by the Customer.

6.5. The Customer hereby covenants that it will comply, and that it shall procure that its Users comply, with Cyber Risk Aware's policies and procedures as set forth in the Cyber Risk Aware Operational Procedures Manual (attached at Exhibit B), and all applicable laws in connection with the Customer and its Users' use of the Software and the Communications Materials.

6.6. The Customer (and its Users) shall be solely responsible for the accuracy of their respective Customer Content. Each of the Customer and the User shall be responsible for obtaining all required rights and licences to use and display its own Customer Content in connection with its or their respective use of the Software and the Communications Materials.

6.7. The Customer acknowledges that the Services are designed to assist the Customer and its Users in developing customised fake phishing e-mail campaigns for purposes of employee training. The Customer shall be solely responsible for the Customer's and its Users' compliance with all applicable laws and governmental regulations, and any results in connection with the Customer's or its Users' use of the Services (including any reports or information produced in connection therewith).

6.8. The Customer shall be liable to Cyber Risk Aware for all acts and omissions of its Users as if that of the Customer for the purposes of this Agreement.

6.9. The Customer shall keep the administrative credentials (e.g. usernames and passwords) provided by Cyber Risk Aware and/or chosen by the Customer or a User in connection with its use of the Services confidential and not disclose any such credentials to any third party. In addition, the Customer shall notify Cyber Risk Aware immediately upon the disclosure of any such credentials. Upon any termination of the engagement of any employee with administrative credentials, the Customer shall must ensure that such credentials are expired and removed.

6.10. Cyber Risk Aware is not responsible for:

6.10.1. the Customer's or its Users access to the Internet;

6.10.2. interception or interruptions of communications through the Internet; or

6.10.3. changes or losses of data through the Internet.

6.11. With the Customer's prior written consent:

6.11.1. Cyber Risk Aware may refer to the Customer on its website and in other marketing material, including but not limited to a possible joint press release coinciding with the launch of the Software by the Customer; and

6.11.2. the Customer agrees to provide Cyber Risk Aware with the Customer's logo for possible use in marketing material where the Customer is referred to as a Cyber Risk Aware customer.

6.12. In the event the Customer is licencing On-Site Software, at Cyber Risk Aware's written request, the Customer will furnish Cyber Risk Aware with a certification signed by an authorised signatory of the Customer verifying that the On-Site Software is being used pursuant to the terms of this Agreement.

6.13. For a period of two years after the expiration of this Agreement, the Customer shall maintain on its premises copies of all records and licences relevant to this Agreement. In the event Customer does not renew the licence to the On-Site Software, the Customer will uninstall the On-Site Software and certify to Cyber Risk Aware, in writing by an authorised signatory, that all On-Site Software has been uninstalled.

7. TERM AND TERMINATION

7.1. This Agreement shall commence on the Effective Date and, unless terminated earlier in accordance with this Agreement, shall continue for the Term and for any Renewal Term for which the Customer pays the Renewal Subscription Fee in accordance with this Agreement.

7.2. The initial term of the Licence is that which is set forth in the Ordering Document (together with any period of extension under Section 7.2 hereof, the "Term"). The Agreement is not cancellable and shall remain in effect until it expires or is earlier terminated according to its terms. ("**Term**").The Licence to the Software shall automatically renew, unless otherwise terminated in accordance with the provisions of this Agreement for additional one (1) year terms (each a "**Renewal Term**") unless the Customer notifies Cyber Risk Aware, in writing, of its intention not to renew at least sixty (60) days prior to:

7.2.1. the expiration of the Term; or

7.2.2. the expiration of any Renewal Term.

7.3. Upon each Renewal Term, the Customer shall:

7.3.1. subject to receipt of invoice, pay within thirty (30) days prior to the expiration of the Initial Term or any subsequent Renewal Term to Cyber Risk Aware, the renewal subscription fee of at Cyber Risk Aware's list price, subject to any applicable discounts ("**Renewal Subscription Fee**");

7.3.2. be entitled to request changes/modifications to the Software and where such changes and work scope are agreed, Cyber Risk Aware shall be entitled to charge the Customer a fee in addition to the Renewal Subscription Fee for such changes/modifications.

7.4. Either Party may terminate this Agreement immediately by written notice to the other Party if the other Party commits a breach of this Agreement which such other Party fails to remedy (if remediable) within 30 days after the service of written notice requiring it to do so. A breach by a User shall be considered a breach by the Customer for the purposes of this Agreement.

7.5. Upon termination of this Agreement for any reason:

7.5.1. all rights granted to the Customer under this Agreement shall cease;

7.5.2. the Customer and its Users must immediately cease all activities authorised by Agreement; and

7.5.3. the Customer must immediately delete or remove the Software from all computer equipment in the Customer's possession, and immediately destroy or return to Cyber Risk Aware (at Cyber Risk Aware's option) all copies of the Software, the Communications Materials and the Documentation then in the Customer's possession, custody or control and, in the case of destruction, certify to Cyber Risk Aware that it has done so.

7.6. In the event of a Material Breach of this Agreement by the Customer or by Cyber Risk Aware, Cyber Risk Aware or the Customer may immediately terminate this Agreement by written notice to the defaulting Party.

7.7. Upon any termination, the Customer's and its Users' right to use and access the Services (including the Software), the Communications Materials and the Documentation shall be terminated.

8. CONFIDENTIALITY

8.1. The parties acknowledge that the Software, Documentation, Customer Content and other confidential information (collectively the "**Confidential Information**") that may be provided by one party or its authorised representative (the "**Disclosing Party**") to the other (the "**Receiving Party**") is confidential information of the Disclosing Party.

8.2. The Receiving Party agrees not to disclose the Confidential Information to third parties or use the Confidential Information other than in connection with this Agreement. The Receiving Party will use at least the same security measures it uses to protect its own confidential and trade secret information but no less than reasonable measures to protect the Confidential Information.

8.3. Confidential Information shall not include information:

8.3.1. already in the Receiving Party's possession at the time of disclosure without an obligation of confidentiality;

8.3.2. that is or later becomes part of the public domain through no fault of the Receiving Party; or

8.3.3. that is required to be disclosed pursuant to law or court order provided that the Receiving Party shall notify the Disclosing Party prior to such required disclosure, if permitted by law, and assist Disclosing Party in preventing or limiting such required disclosure.

8.4. The Receiving Party agrees and acknowledges that any breach of the provisions regarding ownership or confidentiality contained in this Agreement may cause the Disclosing Party

irreparable harm and the Disclosing Party may seek to obtain injunctive relief as well as seek all other remedies available to Disclosing Party in law and in equity in the event of breach or threatened breach of such provisions.

8.5. Notwithstanding the above, Cyber Risk Aware may anonymise and aggregate data from the Customer for the purposes of analysis and reporting, provided that none of the individual data is able to be identified as received from the Customer or any of its Users.

8.6. Each party shall exercise its rights and perform its obligations under this Agreement in accordance with all applicable laws including the Data Protection Legislation. The parties acknowledge that certain of the Confidential Information may be Customer Content which constitutes personal data.

9. DATA PROTECTION

9.1. Both parties will comply with all applicable requirements of the Data Protection Legislation. This clause 9 is in addition to, and does not relieve, remove or replace, a party's obligations or rights under the Data Protection Legislation.

9.2. The parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the controller and the Cyber Risk Aware is the processor. Exhibit D sets out the scope, nature and purpose of processing by Cyber Risk Aware, the duration of the processing and the types of personal data and categories of data subject.

9.3. Without prejudice to the generality of clause 9.1, the Customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the personal data to Cyber Risk Aware for the duration and purposes of this agreement.

9.4. Without prejudice to the generality of clause 9.1, Cyber Risk Aware shall, in relation to any personal data processed in connection with the performance by Cyber Risk Aware of its obligations under this agreement:

9.4.1. process that personal data only on the documented written instructions of the Customer unless Cyber Risk Aware is required by Applicable Law to otherwise process that personal data. Where Cyber Risk Aware is relying on the laws of a member of the European Union or European Union law as the basis for processing personal data, Cyber Risk Aware shall promptly notify the Customer of this before performing the processing required by the Applicable Law unless the Applicable Law prohibits Cyber Risk Aware from so notifying the Customer;

9.4.2. ensure that it has in place appropriate technical and organisational measures, reviewed and approved by the Customer, to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting personal data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to personal data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it);

9.4.3. ensure that all personnel who have access to and/or process personal data are obliged to keep the personal data confidential; and

9.4.4. not transfer any personal data outside of the European Economic Area unless the prior written consent of the Customer has been obtained and the following conditions are fulfilled:

(a) the Customer or Cyber Risk Aware has provided appropriate safeguards in relation to the transfer;

(b) the data subject has enforceable rights and effective legal remedies;

(c) Cyber Risk Aware complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any personal data that is transferred; and

(d) Cyber Risk Aware complies with reasonable instructions notified to it in advance by the Customer with respect to the processing of the personal data;

9.4.5. assist the Customer, at the Customer's cost, in responding to any request from a data subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

9.4.6. notify the Customer without undue delay on becoming aware of a personal data breach;

9.4.7. at the written direction of the Customer, delete or return personal data and copies thereof to the Customer on termination of the agreement unless required by Applicable Law to store the personal data; and

9.4.8. maintain complete and accurate records and information to demonstrate its compliance with this clause 9 and immediately inform the Customer if, in the opinion of Cyber Risk Aware, an instruction infringes the Data Protection Legislation.

9.5. The Customer consents to Cyber Risk Aware appointing a third party processor to process Personal Data under this agreement. Cyber Risk Aware confirms that it has entered or (as the case may be) will enter with the third party processor into a written agreement incorporating terms which are substantially similar to those set out in this clause 9 which Cyber Risk Aware confirms reflect and will continue to reflect the requirements of the Data Protection Legislation. As between the Customer and Cyber Risk Aware, Cyber Risk Aware shall remain fully liable for all acts or omissions of any third party processor appointed by it pursuant to this clause 9.

10. INDEMNIFICATION

10.1. The Customer shall indemnify, defend, and hold Cyber Risk Aware harmless against any and all losses, damages, claims, or liabilities of any nature that are incurred by Cyber Risk Aware (including reasonable attorneys' fees) arising out of the Customer's and/or its User's use of the Services (including the Software), the Communication Materials and the Documentation other than in accordance with the terms of this Agreement.

10.2. Subject always to the exclusions and limitations of liability set out herein, Cyber Risk Aware shall indemnify, defend, and hold the Customer harmless against any and all losses, damages, claims, or liabilities suffered or incurred by the Customer to the extent arising or based upon (a) any negligent act of Cyber Risk Aware, including any data breach or cyber security incident to the extent caused by the negligence of Cyber Risk Aware, or (b) a third party claim that the Customer's use of the Services (including the Software), the Communications Materials and/or the Documentation in accordance with the terms of this Agreement provided by Cyber Risk Aware hereunder, infringes a valid patent or copyright

registered anywhere in the world. Cyber Risk Aware's obligations under this clause 10.2 are also contingent upon:

10.2.1. the Customer providing Cyber Risk Aware with prompt written notice of such claim;

10.2.2. the Customer providing reasonable cooperation to Cyber Risk Aware in Cyber Risk Aware's defense of any such claim; and

10.2.3. the Customer granting to Cyber Risk Aware lead authority and lead control over the defense and settlement of such claim, taking into account all submissions of the Customer in that regard.

10.3. Neither party shall settle any claim in a manner that results in admission of any liability by the other party or places any ongoing restrictions on the other party without the other party's prior written consent, such consent shall not be unreasonably withheld.

10.4. If Software and/or Communications Materials licenced to the Customer hereunder becomes, or in Cyber Risk Aware's opinion is likely to become, the subject of a claim of infringement, Cyber Risk Aware may, at its option:

10.4.1. procure for the Customer and its Users the right to continue to use the Software and/or Communications Materials;

10.4.2. replace or modify the Software and/or Communications Materials to make it non-infringing; or

10.4.3. terminate this Agreement.

11. LIMITED WARRANTY

11.1. Cyber Risk Aware warrants that:

11.1.1. the Software will, when properly used and on an operating system for which it was designed, perform substantially in accordance with the functions described in the Documentation; and

11.1.2. that the Documentation correctly describe the operation of the Software in all material respects, for a period of 90 days from the date the Customer and/or its Users are granted initial access to the Software ("**Warranty Period**").

11.2. If, within the Warranty Period, the Customer notifies Cyber Risk Aware in writing of any defect or fault in the Software as a result of which it fails to perform substantially in accordance with the Documentation, Cyber Risk Aware will use all reasonable endeavours to repair or replace the Software.

11.3. The warranty does not apply:

11.3.1. if the defect or fault in the Software results from the Customer and/or its Users or any person other than Cyber Risk Aware having altered or modified the Software;

11.3.2. if the defect or fault in the Software results from the Customer or its Users having used the Software in breach of the terms this Agreement; and

11.3.3. claims that are not reported to the Cyber Risk Aware within the Warranty Period.

12. LIMITATION OF LIABILITY AND DISCLAIMER OF WARRANTIES

12.1. The Customer acknowledges that the Services (including the Software) has not been developed to meet the Customer's and/or its Users individual requirements, and that it is therefore the Customer's responsibility to ensure that the facilities and functions of the Services as described in the Documentation meet the Customer's requirements.

12.2. Cyber Risk Aware only supply the Services (including the Software), Communications Materials and the Documentation for internal use by the Customer's business, and the Customer shall not use the Services (including the Software), Communications Materials and the Documentation for any re-sale purposes. Cyber Risk Aware shall not in any circumstances whatever be liable to the Customer or its Users, whether in contract, tort (including negligence), breach of statutory duty, or otherwise, arising under or in connection with this Agreement for:

12.2.1. loss of profits, sales, business, or revenue;

12.2.2. business interruption;

12.2.3. loss of anticipated savings;

12.2.4. loss or corruption of data or information;

12.2.5. loss of business opportunity, goodwill or reputation; or

12.2.6. any indirect, incidental, special, pecuniary or consequential loss or damage.

12.3. The Customer's sole remedy and Cyber Risk Aware's sole obligation in the event of breach of the warranty for the Software is the repair or replacement of the Software in accordance with clause 11.2.

12.4. The Customer shall be liable to Cyber Risk Aware in respect of any liability to the extent arising due to the negligent act of a User.

12.5. Subject to the terms of this Agreement and save as provided in clause 12.6, each party's total liability to the other in respect of any and all claims, whether in contract, tort (including negligence), breach of statutory duty, or otherwise, arising under or in connection with this Agreement or any collateral contract, shall in no circumstances exceed a sum equal to the aggregate Fees paid by the Customer to Cyber Risk Aware under this Agreement in the twelve (12) months preceding the event which gave rise to the claim. The limitation of liability set out in this clause 12.5 shall not apply in respect of any liability arising due to a breach of the obligations of confidentiality set out under this Agreement or any violation of the other party's Intellectual Property Rights, including any Material Breach.

12.6. Subject to the terms of this Agreement, the total liability of Cyber Risk Aware, in respect of any and all claims, whether in contract, tort (including negligence), breach of statutory duty, or otherwise, to the extent arising due to a breach by Cyber Risk Aware of the Data Protection Legislation, including, for the avoidance of doubt, under the indemnity at clause 10.2 above, shall in no event exceed one million Euro (€1,000,000).

12.7. This Agreement sets out the full extent of Cyber Risk Aware's obligations and liabilities in respect of the Services (including the Software), the Communications Materials, the Documentation and the Support Services. Except as expressly stated in this Agreement, there are no conditions, warranties, representations or other terms, express or implied, that are binding on Cyber Risk Aware. Any condition, warranty, representation or other term concerning the Services (including the Software), Communications Materials, the Documentation and the Support Service which might otherwise be implied into, or incorporated in, this Agreement whether by statute, common law or otherwise, is excluded to the fullest extent permitted by law.

12.8. THE SERVICES (INCLUDING THE SOFTWARE), THE COMMUNICATIONS MATERIALS AND THE DOCUMENTATION ARE PROVIDED ON AN "AS IS" BASIS. THE CUSTOMER ACKNOWLEDGES THAT ACCESS TO THE SERVICES MAY BE DISRUPTED OR ACCESS TO THE SOFTWARE MAY BE UNAVAILABLE FOR REASONS BEYOND CYBER RISK AWARE'S CONTROL, INCLUDING BUT NOT LIMITED TO ISSUES RELATED TO THE HOSTING ENVIRONMENT FOR THE SOFTWARE. CYBER RISK

AWARE DOES NOT GUARANTEE ACCESS TO THE SERVICES OR THAT THE SERVICES WILL PERFORM TO ANY PERFORMANCE REQUIREMENTS.

12.9. CYBER RISK AWARE DISCLAIMS ALL OTHER REPRESENTATIONS, WARRANTIES, AND CONDITIONS RELATED TO THE SERVICES (INCLUDING THE SOFTWARE), ACCESS TO THE SERVICES (INCLUDING THE SOFTWARE), THE COMMUNICATIONS MATERIALS, THE DOCUMENTS AND THE SUPPORT SERVICES, WHETHER EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, ACCURACY WITH RESPECT TO THE DOCUMENTATION, AND WARRANTIES ARISING FROM COURSE OF DEALING OR USAGE OF TRADE.

12.10. Nothing in this Agreement shall limit or exclude a party's liability for:

12.10.1. death or personal injury resulting from party's negligence;

12.10.2. fraud or fraudulent misrepresentation;

12.10.3. any other liability that cannot be excluded or limited by Irish law.

13. **NOTICES**

Any notice required or permitted to be made or given by either party pursuant to this Agreement shall be in writing and shall be deemed sufficiently made and given if sent to the other party, via certified or registered mail, or other express mail service, to the most recent known address of a party.

14. **MISCELLANEOUS**

14.1. The Services, the Licence and the provision of the Support Services is expressly conditioned on the Customer's acceptance of the terms and conditions expressed herein and Cyber Risk Aware hereby rejects any additional or different terms in Customer's response to this offer.

14.2. This Agreement, together with all Exhibits, represents the final expression and the complete and exclusive statement of the agreement between the parties and supersedes any other agreement or understanding, oral or written on the subject matter. If there is an inconsistency between any of the provisions in the main body of this Agreement and the Exhibits, the provisions in the main body of this Agreement shall prevail.

14.3. In no event shall any oral representations made by any party, including any employee or agent of Cyber Risk Aware, be considered part of this Agreement or apply to the Services, the Software, the Documentation, the Communications Materials or the Support Services provided by Cyber Risk Aware. By accepting the terms of this Agreement, the Customer agrees that in the event the Customer's purchase order or any other form contains terms additional to or different from those set forth herein, Cyber Risk Aware expressly rejects any additional or different terms and that the agreement between Cyber Risk Aware and the Customer shall be exclusively governed by the terms of this Agreement.

14.4. The Customer acknowledges that the Software, the Documentation and/or the Communications Materials may be subject to the laws and export regulations of Ireland, and the Customer agrees to comply with all such laws and regulations.

14.5. This Agreement may not be assigned or transferred by the Customer without the prior written consent of Cyber Risk Aware. This Agreement may not be modified or amended except by an instrument in writing signed by the parties hereto. Any failure of either party to enforce any of the provisions of this Agreement will not be construed as a waiver of such provisions or the right of the party thereafter to enforce each and every such provision. In the event any provision of this Agreement is found to be invalid or unenforceable, the parties hereby agree that the court shall enforce such provision to the extent permitted by law and,

to the extent such provision is not enforceable, shall enforce the remainder of this Agreement as if such provision were not included in this Agreement.

14.6. The terms of clauses 2.4 (intellectual property), 6 (Customer Obligations), 8 (Confidentiality), 12 (Limitation of Liability and Disclaimer of Warranties), and 14 (Miscellaneous) will survive termination or expiration of this Agreement for any reason.

14.7. This Agreement shall be governed by the laws of Ireland, without regard to its conflicts of laws provisions and the parties irrevocably submit to the non-exclusive jurisdiction of the courts of Ireland. The terms of the U.N. Convention on Contracts for the International Sale of Goods shall not apply. This Agreement may be executed in counterparts, each of which shall be deemed an original and all of which, taken together, shall constitute one and the same instrument.

Version: January 12th , 2021

EXHIBIT B

Cyber Risk Aware Operational Procedures Manual (Version 1.2)

Section 1 - Before You Get Started:

Prior to using any of Cyber Risk Aware's solutions, users should carefully familiarise themselves with the most recent online help tutorials and instructioanl demonstration videos. Updated versions of this support content will be regularly provided by Cyber Risk Aware.

Familiarise yourself with this Manual and Comply with Applicable Law

Cyber Risk Aware has authorised the Customer and its Users to use of the Security Training Platform under a Subscription Agreement or other services agreement. Please ensure that any Customer personnel given access to the Security Training Platform system have fully familiarised themselves with the most current version of the Cyber Risk Aware Operations Manual.

Whitelist Cyber Risk Aware's Email Servers

Cyber Risk Aware recommends whitelisting the IP addresses of the Security Training Platform email servers, so that simulated phishing emails can pass through any email filters your organisation may have. To obtain a list of IP addresses please contact your Cyber Risk Aware Customer Support person.

Inform Your IT department, Security Office, and Help Desk of Training Campaigns

Inform relevant parties in your organisation about training assignments and simulated attacks that will be delivered to your end users before starting a new campaign. This step is necessary to prevent any potential misunderstanding, for example, filtering out training or simulated attack emails accidentally or preventing access to online training materials.

Start Slowly

Cyber Risk Aware recommends that you conduct a small pilot campaign before sending one to your entire organisation. This will help to familiarise you with our system and reduce unintended mistakes.

Contact Cyber Risk Aware for Help or Questions

If you have questions, please email us at support@cyberriskaware.com

Section 2 - Security Training Platform:

Cyber Risk Aware's Security Training Platform is an online Software-as-a-Service tool developed by Cyber Risk Aware. The Security Training Platform includes software training modules, User assessments, administrative capabilities, and reporting to implement a security awareness program. The Security Training Platform allows organisations to test the readiness of their workforce and teach users to better protect themselves against cyber security threats.

Specifically, the Security Training Platform has been designed to enable security and IT personnel at an organisation to easily implement a program to train their end users by selecting training modules and user assessments to be delivered to some or all of their users.

The Security Training Platform has been designed to be easy to use with self-explanatory steps. This document outlines the overall processes for creating effective training campaigns.

Securely Manage Security Training Platform Credentials

Please apply best practices in securely managing administrative credentials (i.e. usernames and passwords) required to access the Security Training Platform.

Verify Your Email Addresses

The Security Training Platform should only be used to make training or assessment assignments to email addresses within email domains of each client as described in Exhibit A of your Cyber Risk Aware Subscription Agreement or End User Licence Agreement. Before adding a contact into the system it is your responsibility to verify that the email address is correct, that it corresponds to an employee of your organisation, and that sending training to the individual does not violate any of your organisation's policies or applicable law.

Provide Your IT Department, Security Office, and Help Desk Personnel with a Response to Inquirers

When receiving training, some members of your organisation may contact your IT Department, Security Office, Help Desk or some equivalent part of your organisation, asking about the training. You will need to let personnel at these offices know what to say to people who ask.

Section 3 - Simulated Attack Training Campaigns:

PhishMaestro is an online Software-as-a-Service tool developed by Cyber Risk Aware Limited. This tool allows organisations to test the readiness of their workforce and teach people to better protect themselves against phishing emails.

Specifically, PhishMaestro has been designed to enable security/IT personnel at an organisation to easily select and customise fake phishing email attack campaigns they can then deliver to some or all of their users. While preparing a simulated phishing campaign, security/IT personnel at the organisation can also choose from a number of customizable training interventions, which will be shown to users who fall for the simulated attack.

The PhishMaestro tool has been designed to be easy to use with self-explanatory steps. This document outlines the overall processes for creating an effective PhishMaestro campaign.

Securely Manage PhishMaestro Credentials

Please apply best practices in securely managing administrative credentials (i.e. usernames and passwords) required to access the PhishMaestro tool.

Verify Your Email Addresses

PhishMaestro should only be used to send emails to email domains listed in Exhibit A of your Cyber Risk Aware Subscription Agreement or End User Licence Agreement. Before adding a contact into the system it is your responsibility to verify that the email address is correct, that it corresponds to a user within your organisation, and that sending a fake phishing email to the individual does not violate any of your organisation's policies or applicable law. The PhishMaestro service will only allow you to send emails to your company email domains and not to any personal or other company email addresses.

Inform Your IT department, Security Office, and Help Desk of Email Campaigns

Inform relevant parties in your organisation about simulated phishing emails that will be sent from PhishMaestro before starting a campaign. This step is necessary to prevent any potential misunderstanding, for example, filtering out PhishMaestro training emails accidentally or preventing access to PhishMaestro training materials.

Provide Your IT Department, Security Office, and Help Desk Personnel with a Response to Inquirers

When receiving a simulated phishing email, some members of your organisation may contact your IT Department, Security Office, Help Desk or some equivalent part of your organisation, asking if the PhishMaestro simulated phishing emails are real. You will need to let personnel at these offices know what to say to people who ask. Your options are either to tell inquirers that this is (1) an authorised training campaign, or (2) to be generally careful about phishing emails. The latter option will reduce the chance users talk to one another about what they received, will likely result in a more effective campaign, and will likely give you a more accurate assessment of the readiness of your workforce.

Use Content You Own and Control

Using content, including images that your organisation has not created or does not control, is potentially risky. Doing so can result in malware, viruses, or other malicious software being inadvertently installed on your users' computers. It could also result in users submitting sensitive information to a real phishing site. You may not have the legal right of use such content or images and use could result in liability to your organisation.

As such, when you create your own or customise a simulated phishing email or a simulated phishing login page, it is best for you to use content that has been created internally within the organisation.

EXHIBIT C

Service Level Agreement (SLA)
by
Cyber Risk Aware

Document Owner:	Customer Support, Cyber Risk Aware Limited

1. Agreement Overview

This Agreement remains valid until superseded by a revised agreement mutually endorsed by the stakeholders. This Agreement outlines the parameters of all IT services covered as they are mutually understood by the primary stakeholders. This Agreement does not supersede current processes and procedures unless explicitly stated herein.

2. Goals & Objectives

The **purpose** of this Agreement is to ensure that the proper elements and commitments are in place to provide consistent IT service support and delivery to the Customer(s) by the Service Provider(s).

The **goal** of this Agreement is to obtain agreement for IT service provision between the Service Provider(s) and Customer(s).

The **objectives** of this Agreement are to:

- Provide clear reference to service ownership, accountability, roles and/or responsibilities.
- Present a clear, concise and measurable description of service provision to the customer.
- Match perceptions of expected service provision with actual service support & delivery.

3. Stakeholders

The following Service Provider(s) and Customer(s) will be used as the basis of the Agreement and represent the **primary stakeholders** associated with this SLA:

IT Service Provider(s): Cyber Risk Aware Limited. ("Provider")
IT Customer(s): "**Licensee**"

4. Periodic Review

This Agreement is valid from the **Effective Date** outlined herein and is valid until further notice. This Agreement should be reviewed at a minimum once per fiscal year; however, in lieu of a review during any period specified, the current Agreement will remain in effect.

The **Business Relationship Manager** ("Document Owner") is responsible for facilitating regular reviews of this document. Contents of this document may be amended as required, provided mutual agreement is obtained from the primary stakeholders and communicated to all affected parties. The Document Owner will incorporate all subsequent revisions and obtain mutual agreements / approvals as required.

Business Relationship Manager: Customer Support Team
Review Period: Yearly

5. Service Agreement

The following detailed service parameters are the responsibility of the Service Provider in the ongoing support of this Agreement.

5.1. Service Scope

The following Services are covered by this Agreement, as part of technical support we will;

- provide support on standard functionality and Software Product defects. It does not include the provision of customisation advice or consulting services. Neither does it cover problems caused by your system administrator, such as your accidental or inadvertent destruction of your own data, or a Force Majeure
- provide monitored email support
- provide monitored Ticketing System Support

5.2. Customer Requirements

Customer responsibilities and/or requirements in support of this Agreement include:

- Reasonable availability of customer representative(s) when resolving a service related incident or request.

5.3. Service Provider Requirements

Service Provider responsibilities and/or requirements in support of this Agreement include:

- Meeting response times associated with service related incidents.
- Appropriate notification to Customer for all scheduled maintenance.

5.4. Service Assumptions

Assumptions related to in-scope services and/or components include:

- Changes to services will be communicated and documented to all stakeholders.

6. Service Management

Effective support of in-scope services is a result of maintaining consistent service levels. The following sections provide relevant details on service availability, monitoring of in-scope services and related components.

6.1. Service Availability

As part of the Hosted Service, Cyber Risk Aware will use commercially reasonable efforts to provide Customer administrators with online availabilty to Cyber Risk Aware 99.8% (ninety-nine and eight tenths percent) of the time in any calendar month "Uptime", excluding downtime caused by Scheduled Maintenance, force majeure events, or acts or ommisions of Customer not in accordance with the Software License agreement and documentation.

6.2. ***Service Credit***

Service Credits are a remedy for any performance or online availability to Cyber Risk Aware under the Agreement and this SLA

"**Maximum Available Minutes**" is the average number of minutes per month, forty-four thousand (44,000) during a given Cyber Risk Aware annual subscription license period.

Downtime: The total accumulated Minutes per month, during a given Cyber Risk Aware annual subscription license period, in which the Cyber Risk Aware online system is unavailable excluding any scheduled maintenace. A minute is considered unavailable for Cyber Risk Aware when there is no external connectivity between Cyber Risk Aware and Microsoft's Internet gateway in Azure.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

Monthly Uptime % = (Maximum Available Minutes-Downtime)/(Maximum Available Minutes) x 100

Service level Credit = A * B		
Monthly UPTIME PERCENTAGE	***SERVICE CREDIT % (A)***	***At Risk Amount per Month (B)***
<99.8%	***10%***	***10% of (Annual Subscription fee / 12)***
<99%	***25%***	***25% of (Annual Subscription fee / 12)***

Limitations
This SLA and any applicable Service Levels do not apply to any performance or availability issues:

1. Due to factors outside our reasonable control (for example, natural disaster, war, acts of terrorism, riots, government action, or a network or device failure external to our data centers, including at your site or between your site and our data center);

2. That result from the use of services, hardware, or software not provided by us, including, but not limited to, issues resulting from inadequate bandwidth or related to third-party software or services;
3. Caused by your use of a Service after we advised you to modify your use of the Service, if you did not modify your use as advised;
4. During or with respect to preview, pre-release, beta or trial versions of a Service, feature or software (as determined by us);
5. That result from your unauthorized action or lack of action when required, or from your employees, agents, contractors, or vendors, or anyone gaining access to our network by means of your passwords or equipment, or otherwise resulting from your failure to follow appropriate security practices;
6. That result from your failure to adhere to any required configurations, use supported platforms, follow any policies for acceptable use, or your use of the Service in a manner inconsistent with the features and functionality of the Service (for example, attempts to perform operations that are not supported) or inconsistent with our published guidance;
7. That result from faulty input, instructions, or arguments (for example, requests to access files that do not exist);
8. That result from your attempts to perform operations that exceed prescribed quotas or that resulted from our throttling of suspected abusive behavior;
9. Due to your use of Service features that are outside of associated Support Windows; or
10. For licenses reserved, but not paid for, at the time of the Incident.

6.3. Support Availability

Coverage parameters specific to the service(s) covered in this Agreement are as follows:

- Emails & Ticketing system are monitored between 8:00 A.M. to 6:00 P.M. Monday – Friday excluding Irish Public Holidays. Emails received & tickets raised outside of office hours will be collected, however no action can be guaranteed until the next working day.
- Tickets can be raised within the portal, using the **Support Request** button along the left-hand side menu ribbon, input the details and click the **Save Support Request** button which raises a ticket in our queue.
- Emailing support@cyberriskaware.com will raise a ticket on your behalf and places it in our queue.
- You will be notified by email or telephone as support tickets move through the process to resolution.
- You are permitted to view the status of the ticket or add comments by creating a log in through our ticketing system.

6.4. Service Related Incidents and/or requests

Classificationof Support tickets are placed into the following categories:

- Support Issue - a question about standard CyberRiskAware functionality that does not involve changes to the core Software Product, although it may involve changes to the configuration of the Portal made by the administrator or the CyberRiskAware Support Staff
- Enhancement Request - request to add functionality to the core Software Product
- Onboarding – Portal Creation, Login Issue, queries around portal setup
- Bug – a defect on the CyberRiskAware Platform

Support Issues can generally be resolved within a few hours of submission based on advice or actions provided by support staff. Enhancement requests may be scheduled at our discretion, based on the perceived usefulness of the request for other customers. We shall respond to and use reasonable commercial efforts to resolve issues deemed to be Bugs in accordance with the priority levels indicated below, priority levels shall be determined in good faith with the Customer.

Priority	Description	Investigation Response Time	Target Resolution/Workaround Time*
Urgent	System Down - The Platform is unavailable to All customers in All Regions	0-30 Min(s)	0-1 hour – we will assign as many engineers and/or support staff as needed 24/7 until the problem is resolved.
High	Functionality of the platform is compromised/certain functions are disabled but the main software remains operable. E.g. Customer is unable to login to the platform.	0-60 Min(s)	0-1 day – we will assign as many engineers and/or support staff as needed along with the best work around available.
Medium	A minor issue which does not affect the customer from performing a task, but rather causes an inconvenience.	0-6 Hour(s)	It will be scheduled for the next regular deployment. If not, a correction will be typically provided within a week.
Low	An issue with negligible impact for the end user experience/general information requests such as usage and configuration/request for a feature that is deemed non-critical	0-24 Hour(s)	The resolution may be made at the discretion of the Provider.

*Resolution times will extend if:

- A fix needs to be deployed out of office hours.
- Cyber Risk Aware cannot get the details needed in a timely manner from the customer to troubleshoot an issue.

EXHIBIT D

Processing, Personal Data and Data Subjects

1. PROCESSING BY THE SUPPLIER

Nature of Processing:
Where you subscribe to our services or enrol in any phishing, smishing or training campaign via our site, we will record when you open phishing emails or SMS text messages, click on test website links, open test email attachments, visit and enter data in test websites, open training enrolment emails, take training courses, complete training courses, take a knowledge assessment quiz and how you answer each question, if you report an actual or suspected phishing email using PhishHuk or if you watch one of our security videos.

Purpose of Processing:
We will only use your personal information when the law allows us to. Most commonly, we will use your personal data in the following circumstances:
• Where we need to perform the contract, we are about to enter into or have entered into with you.
• Where it is necessary for our legitimate interest (or those of a third party) and your interests and fundamental rights do not override those interests.
• Where we need to comply with a legal or regulatory obligation.

We have set out below, in table format, a description of the ways we plan to use your personal data and the legal basis we rely only to do so. We have also identified our legitimate interests where approppriate:

Purpose/Activity	Type of data	Legal basis for processing
To respond to your queries and to provide you with the information you request from us in relation to our Services,	*- Identity Data* *- Technical Data* *- Usage Data*	*- Necessary for our legitimate interests (to respond to new or existing customer queries and grow our business)* *- Performance of a contact with you*
To provide the Services, including but not limited to Cyber Security training	*- Identity Data* *- Technical Data* *- Usage Data*	*- Necessary for our legitimate interests (to respond to new or existing customer queries and grow our business)* *- Performance of a contract with you*
To carry out the Cyber Security training, simulated phishing, smishing, cyber knowledge assessments and forward any phishing email reported by a client staff member using our "PhishHuk" plugin to the clients security team.	*- Identity Data* *- Usage Data* *- Technical Data* *- Reported Data*	*- Performance of a Contract*
To manage our relationship with you, including notifying you about changes to the Services, or our Privacy Policy.	*- Identity Data* *- Technical Data* *- Usage Data*	*- Performance of a contract* *- Necessary to comply with a legal obligation* *- Necessary for our legitimate interests (to keep our records updated and to study how customers use our products and services).*

To provide you with information about services we offer that are similar to those that you have enquired about.	*- Identity Data* *- Technical Data* *- Usage Data*	*- Necessary for our legitimate interests (to develop our products or Services and grow our business)*
Where you have given us your consent to do so, to provide you with information about other services we feel may interest you.	*- Identity Data* *- Technical Data* *- Usage Data*	*- Consent*
To ensure that content is presented in the most effective manner for you and for your computer or device.	*- Identity Data* *- Technical Data* *- Usage Data*	*- Necessary for our legitimate interests (to keep our Site and the Services updated and relevant and to develop and grow our business).*
To administer and protect our business, our Site and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes.	*- Identity Data* *- Technical Data* *- Usage Data*	*- Necessary for our legitimate interests (for running our business and as part of our efforts to keep our Site and the Services safe and secure)*
To use data analytics to improve or optimise our Site, marketing, customer relationships and experiences.	*- Technical Data* *- Usage Data*	*- Necessary for our legitimate interests (to define types of customers for our products and services, to keep our Site and the Services updated and relevant, to develop and grow our business and inform our marketing strategy).*
To measure or understand the effectiveness of advertising we serve to you and others, and, where applicable, to deliver relevant advertising to you.	*- Identify Data* *- Technical Data* *- Usage Data*	*- Necessary for our legitimate interests (to study how customers use our products or Services, to develop them, to grow our business and to inform our marketing strategy).*

Means of Processing:
An online Security Awareness Training and Simulated phishing platform, hosted in Microsoft Azure Data Centres.

Where you subscribe to our services or enrol in any phishing or training campaign via our site, we will record when you open phishing emails, click on test website links, open test email attachments, visit and enter data in test websites, open training enrolment emails, take training courses, complete training courses, take a knowledge assessment quiz and how you answer each question, if you report an actual or suspected phishing email using PhishHuk or if you watch one of our security videosType of Personal Data

2. TYPES OF PERSONAL DATA

The following types of Personal Data are processed under this DP Agreement:

First Name, Last Name, Email Address, Country, Site, Role regarding the training (Manager or Agent), Line of Business (General Staff, Ops, IT or Client Name), RACFID, Completion status of trainings.

Information you give us

Your Data. This is information about you that you give us by filling in forms on our Site or by corresponding with us by phone, e-mail or otherwise. It includes information you provide when you use our Site, or the Services, or report a problem with our Site.
This is information about you that you give us by filling in forms on our site *.cyberriskaware.com ("**our site**") or by corresponding with us by phone, e-mail or otherwise. It includes information you provide when you register to use our site, subscribe to our service, participate in discussion boards or other social media functions on our site, enter a competition, promotion or survey, and when you report a problem with our site. The information you give us may include your name, business address, work e-mail address, department name and phone number, financial and credit card information.
The information you give us may include:

- **Identity Data:** your full name, address, e-mail address, mobile phone number, address, department, country, language, business entity name, business sector, IP address per user, Web Browser version per user, Operating System version per user, Risky User Behaviour Alarm Code and Description, Employee ID number.
- **Financial Data:** your financial data, including bank account details, billing contact email address and VAT number.
- **Reported Data:** a staff member can report an actual or suspected phishing email to the clients own security team using the Cyber Risk Aware provided "PhishHuk" email client plugin; a risky user behaviour alarm code and description from a technical defense integrated with Cyber Risk Aware.

Information we collect about you.

Automatically Collected Information. With regard to each of your visits to our Site we will automatically collect the following information:

- **Technical Data:** technical information, including the Internet protocol (IP) address used to connect your computer to the Internet, your login information, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform, how often you use the application and other performance data;] and

- **Usage Data:** information about your visit, including the full Uniform Resource Locators (URL), clickstream to, through and from our site (including date and time), products you viewed or

searched for, page response times, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), methods used to browse away from the page, number of reported emails using PhishHuk, number of conducted scheduled and real-time training, phishing, smishing and cyber knowledge assessments, results of conducted scheduled and real-time training, phishing, smishing and cyber knowledge assessments, and any phone number used to call us.

Where you subscribe to our services or enrol in any phishing or training campaign via our site, we will record when you open phishing emails, click on test website links, open test email attachments, visit and enter data in test websites, open training enrolment emails, take training courses, complete training courses, take a knowledge assessment quiz and how you answer each question, if you report an actual or suspected phishing email using PhishHuk or if you watch one of our security videos.

3. CATEGORIES OF DATA SUBJECT

No special categories of personal data.
We do not require or collect any personal data that is sensitive personal data or any special category of personal data under the GDPR.

The following natural persons are subject to this data Processing:

- Data Controller's employees