Services Agreement

Standard Terms

PARTIES

1. Supplier as defined in the Order Form.
2. Customer as defined in the Order Form.

BACKGROUND

A. Supplier is in the business of providing the Services.
B. Customer wishes to receive and Supplier wishes to provide the Services on the terms set out in the Services Agreement.

THE PARTIES AGREE AS FOLLOWS:

1. INTERPRETATION

1. The following definitions and rules of interpretation apply in the Services Agreement:

Applicable Data Protection Laws:

a. To the extent the UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of personal data.
b. To the extent the EU GDPR applies, the law of the European Union or any member state of the European Union to which Supplier is subject, which relates to the protection of personal data.

Applicable Laws: all applicable laws, statutes, regulation and codes from time to time in force in any relevant jurisdiction, including data protection laws other than the Applicable Data Protection Laws, and applicable to the Parties in relation to the Services under the Services Agreement (including without limitation export law and those governing the use of networks, scanners, encryption devices, user monitoring and related software).

Business Day: a day, other than a Saturday, Sunday or UK bank holiday.

Business Hours: the period from 9.00 am to 5:30 pm GMT/BST on any Business Day or as set forth in the Order Form.

Commencement Date: the date of the last signature or as first set forth on the Order Form and agreed by the parties as the effective date of the Services Agreement.

Confidential Information: means any information whether supplied, made available or otherwise accessed or accessible in any form, wholly or in part, and whether or not marked confidential, by either party to the other under or in connection with the Services Agreement and includes (but is not limited to) information relating to software and hardware products, IT infrastructure, samples, equipment, drawings, specifications, information about a party's clients and including customer characteristics and identities, staff and subcontractors to a party including characteristics and identities, trade secrets, technical information and know-how, performance or process data, cost and financial information, market opportunities, business affairs, methods of doing business, strategic marketing, business plans and any information, operation of digital platform, reports or analysis derived from the Confidential Information, but does not information that is or becomes generally available to the public otherwise than as a result of a breach of this agreement, is already available to a receiving party on a non-confidential basis from a third party or is independently developed by a party without relying on Confidential Information supplied by the other party.

Customer: means the party referred to as Customer on the Order Form and any persons, third party agents, subcontractors, consultants, employees and those acting on its behalf.

Customer's Equipment: any equipment, including tools, systems, cabling or facilities, provided by Customer, its agents, employees, subcontractors or consultants which is used directly or indirectly in relation to the supply of the Services including any such items specified in the Order Form or Annex.

Customer Materials: all documents, information, items and materials in any form, whether owned by Customer or a third party, which are provided by Customer to Supplier in connection with the Services, including the items provided pursuant to clause 5.6(d) or otherwise specified in the Services Agreement.

Customer Personal Data: any personal data which Supplier processes in connection with the Services Agreement, in the capacity of a processor on behalf of Customer.

Customer's System: means the system, application and/or network set forth in the Order Form or an Annex which Customer requires to be security tested.

Defense.com Licence: means, where applicable as set forth in the Order Form, a licence granted to Customer for access to and use of the Defense.com Platform and for the provision of the Services and related Deliverables on and via the Defense.com Platform.

Defense.com Platform: means Supplier's online security information and service web portal and/or any other related Supplier facilities or systems to which Customer has been granted access and use as set forth in the Order Form.

Defense.com Users: means in respect of Defense.com Licence, the permitted users who are designated by Customer to use Defense.com Platform.

Deliverables: any output of the Services to be provided by Supplier to Customer as specified in the Order Form or in the Services Agreement Service-specific Terms.

EU GDPR: means the General Data Protection Regulation ((EU) 2016/679), as it has effect in EU law.

Fees: the monetary amounts due for the Services as set forth in the Order Form.

Good Industry Practice: means the exercise of that degree of skill, diligence and foresight which would reasonably and ordinarily be expected from a skilled and experienced service provider engaged in the provision of services similar to the Services under the same or similar circumstances as those applicable to the Services Agreement and which are in accordance with any codes of practice published by relevant trade associations.

Initial Term: the first and minimum Services Agreement duration for any Service as set forth in the Order Form.

Intellectual Property Rights or IPRs: patents, utility models, rights to inventions, copyright and neighbouring and related rights, moral rights, trade marks and service marks, business names and domain names, rights in get-up and trade dress, goodwill and the right to sue for passing off or unfair competition, rights in designs, rights in computer software, data, database rights, rights to use, and protect the confidentiality of, confidential information (including know-how and trade secrets) and all other intellectual property rights, in each case whether registered or unregistered and including all applications 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.

Milestone: a date by which a part or all the Services is to be completed, as set forth in the Order Form.

Monthly Recurring Service Fees: means any monthly recurring fees for the applicable service payable by Customer as detailed on the Order Form.

Order Form(s): shall mean the request on Supplier's standard Order Form from Customer to Supplier for Services to be provided pursuant to the terms of the Services Agreement which agreement, for the avoidance of doubt, applies in each case to a specific Order Form.

Order Form Services Addendum: has the meaning given in clause 7.1.

Professional Services: means consultant delivered Services, as defined by Supplier including, but not limited to, Penetration Testing and compliance Consultancy.

Service(s): means a Supplier service or multiple Supplier services (which may be packaged) that are ordered by Customer as set forth in the Order Form.

Services Agreement: shall mean these Services Agreement Standard Terms together with and which be read to include the Service-specific Terms and a specific Order Form pursuant to which Supplier makes the Services available to Customer, any related Annex and/or any related Order Form Services Addendum.

Supplier's Equipment: any equipment, including tools, systems, documentation, cabling or facilities, provided by Supplier to Customer and used directly or indirectly in the supply of the Services, including any such items specified in the Order Form but excluding any such items which are the subject of a separate agreement between the parties under which title passes to Customer.

Supplier Personal Data: any personal data that Supplier processes in connection with the Services Agreement, in the capacity of a controller.

UK GDPR: has the meaning given to it in section 3(10) as supplemented by section 205(4)) of the Data Protection Act 2018.

VAT: value added tax chargeable in the UK.

2. Clause, Order Form, any Annex and any other Services Agreement headings shall not affect the interpretation of the Services Agreement.
3. A person includes a natural person, corporate or unincorporated body (whether or not having separate legal personality).
4. Any Annex, the Services Agreement Service-specific Terms, the Order Form and/or Order Form Services Addendum forms part of the Services Agreement and shall have effect as if set out in full in the body of these Services Agreement Standard Terms, and any reference to the Services Agreement includes all the above.
5. A reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established.
6. Unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular.
7. Unless the context otherwise requires, a reference to one gender shall include a reference to the other gender.

8. The Services Agreement shall be binding on, and inure to the benefit of, the parties to the Services Agreement and their respective personal representatives, successors and permitted assigns, and references to any party shall include that party's personal representatives, successors and permitted assigns.
9. Unless expressly provided otherwise in the Services Agreement, a reference to legislation or a legislative provision is a reference to it as amended, extended or re-enacted from time to time.
10. A reference to writing or written includes email.
11. Any obligation on a party not to do something includes an obligation not to allow that thing to be done.
12. A reference to the Services Agreement or to any other agreement or document is a reference to this agreement or such other agreement or document, in each case as varied or novated from time to time.
13. References to clauses and the Order Form or any Annex are to the clauses, Order Form and any Annexes of the Services Agreement and references to paragraphs are to paragraphs of the relevant Order Form or Annex.
14. The words including, include, in particular, for example or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those words.

2. STRUCTURE AND SCOPE OF THE SERVICES AGREEMENT

1. The Services Agreement creates a contractual framework between Supplier and Customer under which:
    a. Customer requests from Supplier to provide Services pursuant to the terms of the Services Agreement; and
    b. Supplier agrees to provide the Services pursuant to the terms of the Services Agreement.
2. Each Service specified will be set forth in the Order Form and any applicable Annex.
3. In the event of any conflict or ambiguity, except where otherwise provided, the order of precedence for the Services Agreement shall be as follows:
    a. the applicable Order Form;
    b. the applicable Annex or Order Form Services Addendum; and
    c. the body of these Services Agreement Standard Terms or the Services Agreement Service-specific Terms.

4. The Customer and Supplier may agree to one or more Order Forms, each forming a separate Services Agreement, for the provision of Services.
5. For the Services Agreement to be valid and effective, the Order Form must be confirmed in writing and signed by an authorised representative of each party. Upon signature by both authorised representatives, the Services Agreement shall be binding (and incapable of cancellation other than through the termination provisions contained in clause 13 below) and the Fees and any other charges shall become due as set forth in the Order Form in accordance with the Services Agreement.
6. Each Party warrants to the other Party that it (1) has the full capacity and authority to enter into and perform the Services Agreement and that the Services Agreement is executed by a duly authorised representatives; (2) is the owner, or has the relevant consent from the owner, of all Systems, applications, networks, premises and any other asset that is set out in the Order Form; and (3) will comply with all Applicable Laws.

3. COMMENCEMENT AND DURATION

1. The Services Agreement shall commence on the Commencement Date and shall continue for the Initial Term unless terminated earlier in accordance with clause 13 (Termination). Following the Initial Term of the Services Agreement, where the Services are of the type that can continue and are not specified as not continuing in the Order Form, the Services Agreement shall extend automatically for additional terms of the same duration as the Initial Term (each an "Extension Term") or as otherwise set forth in the Order Form unless terminated on at least 60 days' prior written notice by either party or as otherwise set forth in the Order Form.
2. If there are no incomplete Services under the Order Form as of the date notice to terminate is served under clause 3.1, such notice shall terminate the Services Agreement on the expiry of the notice period and not later than the expiration of the Initial Term or Extension Term, as applicable. Except where provided otherwise or by agreement of the parties, any incomplete Service under the Order Form shall be completed and/or paid for (where completion is not possible due to Customer's failure to perform under the Services Agreement) prior to any termination of the Services Agreement.
3. Customer may procure any of the Services by executing the agreed Order Form with Supplier.

4. Supplier shall provide the Services from the Commencement Date or other date specified in the Order Form.

4. PROVISION OF SERVICES

1. Supplier will provide, and Customer will receive and have use of the Services and any related Deliverables (where applicable, by grant of a Defense.com Licence) in accordance with the Services Agreement for the Initial or Extension Term, as applicable, set out in the Order Form whereby:
    a. each Service and/or Deliverable specified to be provided will be provided in accordance with the Order Form and any applicable Annex; and
    b. Supplier will provide, deliver or otherwise make available such Service and/or Deliverables with Good Industry Practice skill and care, in a timely manner and in accordance with the other provisions of the Services Agreement.
    c. Supplier shall, where it deems appropriate, appoint a contact person in respect of the Services to be performed, such person shall be designated before the delivery of a relevant Service.
    d. Where applicable, Supplier shall observe all health and safety and security requirements that apply at any of Customer's premises and that have been communicated to Supplier under clause 5.6(e), provided that Supplier shall not be liable under the Services Agreement if, as a result of such observation, it is in breach of any of its obligations under the Services Agreement.
    e. Supplier may use a subcontractor, contracted under the Services Agreement terms, to assist with delivery of Services and will carry out the appropriate due diligence to ensure any such subcontractor has the required qualifications and experience to deliver the Services.

5. USE OF THE SERVICE(S)

1. Customer will:
    a. provide to Supplier all necessary co-operation in relation to the Services Agreement including the Order Form and any applicable Annex; and all necessary access to such information as may be required by Supplier to provide the Services including, but not limited to, relevant Customer staff and/or agents, customer data, security access information and configurations services;

b. carry out all customer obligations in a timely and efficient manner;
c. ensure that Customer's Equipment including network and systems comply with the relevant specification and use restrictions provided by Supplier from time to time and comply with any security, information security and technical procedures and requirements in relation to the Services and/or any Deliverables.

2. Customer is responsible for having and maintaining an adequate Customer environment and uninterrupted internet connectivity to receive and/or enable the use of the Services and/or Deliverables. Supplier shall not be liable for any incompatibility, failure, use or misuse by Customer related to Customer's environment.
3. Customer shall not:
    a. infringe any Intellectual Property Rights that belong to or are licensed to Supplier;
    b. create, upload, download, access, store, into the Services and/or any Deliverable any malicious code, programs, viruses, malware or other types of malicious software or material, or links to such software, that are unlawful, insider or confidential information, advertisements or solicitation for any products or services, or could disrupt or harm the operation of such Service and/or Deliverables or incite another to do so; or
    c. copy, reverse engineer, decompile, disassemble or modify a Service and/or any Deliverable or any part, feature, function or user interface thereof, or otherwise reduce to human-perceivable form all or any part of Service and/or any Deliverable, or use or attempt to use any automated program to access any Service and/or any Deliverable, or to search, display, or obtain links to any part of a Service and/or any Deliverable.
4. Customer agrees to indemnify Supplier from any losses suffered, or liabilities incurred because of Customer's breach of clause 5.3.
5. Customer shall not:
    a. knowingly withhold information which may affect Supplier's ability to provide any of the Services and/or Deliverables to Customer or to others (including, where applicable, Defense.com Users), or security or integrity of any of the Services and/or Deliverables;

b. use any Service and/or Deliverable to impersonate any person, or to misrepresent Customer's or any Platform User's identity;
c. engage in sending unsolicited messages to any number or users or via the internet by using any Service and/or Deliverable;
d. use the Service and/or Deliverables in a way which in Supplier reasonable opinion is not within the intended use of such Service or Deliverable;
e. engage in abusive or excessive usage of any Service and/or Deliverable which is usage significantly in excess of average usage patterns, as determined by Supplier, that adversely affects the speed, responsiveness, stability, availability or functionality of any Service and/or Deliverable for other users;
f. make any Service and/or Deliverable available to, or use any Service and/or Deliverable for the benefit of, anyone other than Customer, unless and to the extent expressly stated otherwise in the Order Form;
g. lend, sell, resell, license, sublicense, distribute, make available, rent or lease any Service and/or Deliverable, or include any Service and/or Deliverable in a service or outsourcing offering, unless otherwise agreed in writing with Supplier;
h. access any Service and/or Deliverable to build a competitive solution or service or to benchmark with a non-Supplier service; or
i. use any Service and/or Deliverable in Customer's own products or services, commercially exploit or otherwise make any Service and/or Deliverable available to any third party in any way, unless expressly consented to by Supplier.

6. Customer shall:
    a. co-operate with Supplier as reasonably requested in all matters relating to the Services;
    b. assign a contact person in respect of the Services to be performed under the Order Form, as identified in the Order Form;
    c. provide, for Supplier, its agents, subcontractors, consultants and employees, in a timely manner and at no charge, access to Customer's premises, office accommodation, data and other facilities as reasonably

required by Supplier to carry out the Services, including any such access as is specified in the Order Form;

d. provide to Supplier in a timely manner all documents, information, items and materials in any form (whether owned by Customer or a third party) and meeting attendance by the assigned contact person, project manager and/or any key staff as set forth in the Order Form or otherwise reasonably requested by Supplier in connection with the Services and ensure that they are accurate and complete;
e. inform Supplier in writing of all health and safety and security requirements that apply at any of Customer's premises;
f. ensure that all Customer's Equipment is in good working order and suitable for the purposes for which it is used in relation to the Services and conforms to all relevant Applicable Law requirements or standards;
g. obtain and maintain all necessary licences and consents in accordance with relevant Applicable Law and comply with all relevant legislation as required to enable Supplier to provide the Services;
h. at the request of Supplier, agree to a service review with Supplier once every 6 months or as otherwise reasonably requested; and
i. where applicable as designated in the Order Form, in respect of each Defense.com Licence granted, appoint Defense.com Users, to the maximum number of users as stated in the Order Form, who shall be the only users permitted to access the Defense.com Platform and be provided with the Services and/or Deliverables.

7. If Supplier's performance of its obligations under the Services Agreement is prevented or delayed by any act or omission of Customer, its agents, subcontractors, consultants or employees or any other third-party supplier then, without prejudice to any other right or remedy it may have, Supplier shall be allowed an extension of time to perform its obligations equal to the delay caused by Customer or other third-party supplier or for as long as Supplier deems at its discretion the prevention or delay necessitates.
8. Both Parties shall maintain business continuity and disaster recovery plans to ensure the continuity of the Services in the event of an unforeseen interruption and any other prudent

procedures and measures that are reasonably necessary to prevent the disruption of the Services. Customer shall, in the event of an unforeseen interruption, use best efforts to cooperate with Supplier to ensure the uninterrupted provision of Services.

6. NON-SOLICITATION AND EMPLOYMENT
    1. Each party shall not, without the prior express written consent of the other party, at any time until the expiry of 24 months after the completion of such Services, solicit or entice away from the other party or directly attempt to employ any person who is, or has been, engaged as an employee, consultant or subcontractor of the other party.
7. ORDER FORM SERVICES ADDENDUM
    1. Either party may propose changes to the scope or execution of the Services but no proposed changes shall come into effect until a relevant Order Form Services Addendum has been formally agreed by both parties. The Order Form Services Addendum shall be a document (or email where permitted by Supplier at its sole discretion) citing to the Order Form and setting out the proposed changes and the effect that those changes will have on the Service(s), Fees, any timetable and/or any other Order Form terms.
    2. If Supplier wishes to make a material change to the Services provided to Customer it shall provide a draft Order Form Services Addendum to Customer.
    3. If Customer wishes to make a change to the Services it shall notify Supplier and provide as much detail as Supplier reasonably requires of the proposed changes, including the timing of the proposed change; and Supplier shall, as soon as reasonably practicable after receiving the information, provide a draft Order Form Services Addendum to Customer.
    4. If the parties agree to the Order Form Services Addendum, they shall sign it and that Order Form Services Addendum shall amend the relevant Order Form. If the parties are unable to agree the Order Form Services Addendum, either party may request termination of the affected Service, such termination to take effect as expressly agreed by the parties; however, termination of a Service under this clause shall not affect Customer's payment obligations (as of the date of any such Service termination) under the Services Agreement.
8. FEES, OTHER CHARGES AND PAYMENT

1. In consideration of the administration and allocation of ready resources for the provision of the Services by Supplier, Customer shall pay the Fees upon invoice including where Services cannot be delivered due to Customer's failure to meet any of its obligations under the Services Agreement.
2. Supplier will invoice Customer in accordance with the Order Form or, where not specified in the Order Form, immediately following the Commencement Date of the Order Form on 30-day payment terms.
3. All Services shall be used and, in any event, paid for in full as set forth in this Clause 8 or in the Order Form. Any Services which are unused by Customer during the Initial Term or a relevant Extension Term will expire and shall not be credited, or refunded unless otherwise expressly agreed by the parties in writing.
4. The Fees exclude the following, which shall be payable by Customer monthly in arrears (provided that Supplier has obtained the written consent of Customer, which shall not be unreasonably delayed or withheld), as incurred:
    a. the cost of hotel, subsistence, travelling and any other ancillary expenses reasonably incurred by the individuals whom Supplier engages in connection with the Services; and
    b. the cost to Supplier of any materials or services procured from time to time by Supplier, as it deems appropriate, from third parties for the provision of any Service where such items and their cost are approved by Customer in advance, and for any materials or services reasonably deemed necessary to procure by Supplier, in its absolute discretion, where such items and their costs are notified to Customer in advance.
5. The Fees also exclude services related to non-Supplier delay, cancellation and rescheduling charges, for costs related directly to the administration, system, personnel, facilities, third party and/or other allocated resources associated with scheduled Services. The following charges will apply to any Customer short-term cancellation and rescheduling:
    a. cancellation or rescheduling requested between 7 and 14 days before the scheduled start date for delivery of any Services: 50% of the scheduled Service Fees of the cancelled or rescheduled Service(s); or
    b. for cancellation or rescheduling requested within 7 days before the scheduled start date for delivery of any

Services: 100% of the scheduled Service Fees of the cancelled or rescheduled Service(s).

6. Supplier may choose to increase the Fees on an annual basis with effect from each anniversary of the date of the Services Agreement, to cover, e.g., any increased Supplier costs, in line with the higher of five percent (5%) or the percentage increase in the Consumer Price Index in the preceding 12-month period, and the first such increase shall take effect, at Supplier's discretion, on the first anniversary of the date of the Services Agreement and shall be based on the latest available annual figure for the percentage increase in the Consumer Prices Index.
7. Supplier may, at any time during the Initial Term and during any Extension Term thereafter, vary the Fees payable by Customer by giving at least 30 days prior written notice in the event of new taxation laws, or the introduction or increase in any taxes, levies, costs or expenses, including any taxes, levies which relate to the Services;
8. Supplier will invoice Customer for the Fees as set forth in the Order Form or as set forth in the Services Agreement or as otherwise expressly agreed in writing.
9. Customer shall pay each invoice submitted to it by Supplier based on the following terms:
    a. on 30-day terms where indicated by Supplier or any other terms as set forth on the Order Form;
    b. by credit card on immediate receipt of the invoice;
    c. by direct debit with payments taken 14 days after date of invoice, where credit terms are agreed; or
    d. by payment in advance at any time required by Supplier, where Customer's credit score is insufficient to meet the total value of the contract.
10. Without prejudice to any other right or remedy that it may have, if Customer fails to pay Supplier any sum due under the Services Agreement on the due date:
    a. All sums payable under the Services Agreement for services delivered and to be delivered shall become due and payable by Customer.
    b. Customer shall pay interest on the overdue sum from the due date until payment of the overdue sum, whether before or after a court judgment. Interest under this clause will accrue each day at 4% a year above the Bank of England base rate from time to time, but at 4% a year for any period when that base rate is below 0%; and

c. Supplier may suspend or cancel part or all the Services if payment is not received within 10 days of the due date until payment has been made in full (subject to any other rights and/or remedies under the Services Agreement).

11. All amounts payable to Supplier under the Services Agreement:
    a. are exclusive of any applicable VAT, and Customer shall in addition pay an amount equal to any applicable VAT on those sums on receipt of a VAT invoice; and
    b. shall be paid in full without any set-off, counterclaim, deduction or withholding (other than any deduction or withholding of tax as required by law) and are excluded from Force Majeure clause 15.

9. INTELLECTUAL PROPERTY RIGHTS

1. In relation to the Services and any Deliverables:
    a. Supplier and its licensors shall retain ownership of all IPRs in the Services and the Deliverables, excluding Customer Materials;
    b. Supplier grants Customer, or shall procure the direct grant to Customer of, a fully paid, worldwide, non-exclusive, royalty-free revocable licence during the term of the Services Agreement to copy and modify the Deliverables for the purpose of receiving and using the Services and the Deliverables in its business; and
    c. Customer shall not sub-licence, assign or otherwise transfer the rights granted in clause 9.1(b) to any of its customers or other third parties, unless expressly agreed in writing with Supplier.
2. In relation to Customer Materials, Customer:
    a. and its licensors shall retain ownership of all IPRs in Customer Materials; and
    b. grants to Supplier a fully paid, non-exclusive, royalty-free, non-transferable licence to copy and modify Customer Materials for the term of the Services Agreement, and as required by law thereafter, for the purpose of providing the Services to Customer.
3. Supplier:
    a. warrants that the receipt, use of the Services and the Deliverables by Customer shall not infringe the IPRs of any third party;
    b. shall, subject to Clause 12 (Limitation of Liability), indemnify Customer against all liabilities, costs, expenses, damages and losses suffered or incurred or paid by

Customer arising out of or in connection with any claim brought against Customer for actual or alleged infringement of a third party's Intellectual Property Rights arising out of, or in connection with, the receipt or use of the Services and Deliverables;

c. shall not be in breach of the warranty at clause 9.3(a), and Customer shall have no claim under the indemnity at clause 9.3(b), to the extent the infringement arises from:
    1. compliance with Customer's specifications or instructions, where infringement could not have been avoided while complying with such specifications or instructions and provided that Supplier shall notify Customer if it knows or suspects that compliance with such specification or instruction may result in infringement.
    2. the use of Customer Materials in the development of, or the inclusion of Customer Materials in, the Services or any Deliverable;
    3. any modification of the Services or any Deliverable, other than by or on behalf of Supplier as authorised by Supplier; and

4. Customer:
    a. warrants that the receipt and use in the performance of the Services Agreement by Supplier, its agents, employees, subcontractors or consultants of Customer Materials shall not infringe the rights, including any Intellectual Property Rights, of any third party; and
    b. shall indemnify Supplier against all liabilities, costs, expenses, damages and losses suffered or incurred or paid by Supplier arising out of or in connection with any claim brought against Supplier, its agents, employees, subcontractors or consultants for actual or alleged infringement of a third party's Intellectual Property Rights, to the extent that the infringement or alleged infringement arises out of, or in connection with, the receipt or use of Customer Materials in the performance of the Services Agreement.
5. If either party (Indemnifying Party) is required to indemnify the other party (Indemnified Party) under this clause 9, the Indemnified Party shall:
    a. notify the Indemnifying Party in writing of any claim against it in respect of which it wishes to rely on the

indemnity at clause 9.3(b) or clause 9.4(b) (as applicable) (IPRs Claim);

b. allow the Indemnifying Party, at its own cost, to conduct all negotiations and proceedings and to settle the IPRs Claim, provided that the Indemnifying Party shall obtain the Indemnified Party's prior approval of any settlement agreement, such not to be unreasonably withheld, delayed, or conditioned;
c. provide the Indemnifying Party with such reasonable assistance regarding the IPRs Claim as is required by the Indemnifying Party, subject to reimbursement by the Indemnifying Party of the Indemnified Party's costs so incurred; and
d. not, without prior consultation with the Indemnifying Party, make any admission relating to the IPRs Claim or attempt to settle it, provided that the Indemnifying Party considers and defends any IPRs Claim diligently, using counsel and in such a way as not to bring the Indemnified Party's reputation into disrepute.

6. https://www.lawinsider.com/clause/publicity-and-use-of-trademarks Neither Party shall use any Intellectual Property Rights except with express prior written consent, which consent shall not be unreasonably withheld.

10. DATA PROTECTION

1. For the purposes of this clause 10, controller, processor, data subject, personal data, personal data breach and processing shall have the meaning given to them in the UK GDPR.
2. Both parties will comply with all applicable requirements of Applicable Data Protection Laws. This clause 10 is in addition to, and does not relieve, remove or replace, a party's obligations or rights under Applicable Data Protection Laws.
3. Customer consents to, (and shall procure all required consents, from its personnel, representatives and agents, in respect of) all actions taken by Supplier in connection with the processing of Customer Personal Data, provided these are in compliance with the then-current version of Supplier's privacy policy available at https://www.bulletproof.co.uk/privacy-notice (Privacy Policy). In the event of any inconsistency or conflict between the Privacy Policy and the Services Agreement, the Privacy Policy will take precedence.

4. Customer will ensure that it has all necessary consents and notices in place to enable lawful transfer of Customer Personal Data to Supplier for the duration and purposes of the Services Agreement.
5. Without prejudice to the generality of clause 10.2, Supplier shall, in relation to Customer Personal Data:
    a. process that Customer Personal Data only on the documented instructions of Customer unless Supplier is required by Applicable Laws to otherwise process that Customer Personal Data (Purpose). Where Supplier is relying on Applicable Laws as the basis for processing Customer Personal Data, Supplier shall notify Customer of this before performing the processing required by the Applicable Laws unless those Applicable Laws prohibit the Supplier from so notifying Customer on important grounds of public interest. Supplier shall inform Customer if, in the opinion of Supplier, the instructions of Customer infringe Applicable Data Protection Laws;
    b. implement technical and organisational measures to protect against unauthorised or unlawful processing of Customer Personal Data and against accidental loss or destruction of, or damage to, Customer Personal Data, which Customer has reviewed and confirms are 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;
    c. ensure that any personnel engaged and authorised by Supplier to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory or common law obligation of confidentiality;
    d. assist Customer insofar as this is possible (taking into account the nature of the processing and the information available to Supplier), and at Customer's cost and written request, in responding to any request from a data subject and in ensuring Customer's compliance with its obligations under Applicable Data Protection Laws with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

e. notify Customer without undue delay on becoming aware of a personal data breach involving Customer Personal Data; Where such breach is notifiable to the Information Commissioner's Office (ICO), Supplier shall notify the ICO or other relevant supervisory authority of such breach at the end of any statutorily required notice period where the requisite notice has not been sent earlier either by Customer or Supplier at Customer's instruction;
f. at the written direction of Customer, delete or return Customer Personal Data and copies thereof to Customer on termination of the Services Agreement unless Supplier is required by Applicable Law to continue to process that Customer Personal Data. For the purposes of this clause 10.5(f) Customer Personal Data shall be considered deleted where it is put beyond further use by Supplier;
g. will only process personal data in an identifiable form for no longer than is necessary for the purposes for which it is processed, including but not limited to complying with its obligations under the Payment Card Industry Data Security Standard (PCI DSS) rules which prohibits the storage of payment card verification codes once a transaction has been authorised; and
h. maintain records to demonstrate its compliance with this clause 10, and allow for reasonable audits by Customer or Customer's designated auditor, for this purpose, on reasonable written notice to a maximum of once annually.

6. Customer provides its prior, general authorisation for Supplier to:
    a. appoint processors to process Customer Personal Data, provided that Supplier:
        i. shall ensure that the Services Agreement on which it appoints such processors comply with Applicable Data Protection Laws, and are consistent with the obligations imposed on Supplier in this clause 10;
        ii. shall remain responsible for the acts and omission of any such processor as if they were the acts and omissions of Supplier; and
    b. transfer Customer Personal Data outside of the UK as required for the Purpose, provided that Supplier shall ensure that all such transfers are made in accordance with Applicable Data Protection Laws. For these purposes, Customer shall promptly comply with any reasonable

request of Supplier, including any request to enter into standard data protection clauses adopted by the EU Commission from time to time (where the EU GDPR applies to the transfer) or adopted by the ICO from time to time (where the UK GDPR applies to the transfer).

7. Either party may, at any time on not less than 30 days' written notice, revise this clause 10 by replacing it with any applicable controller to processor standard clauses or similar agreement forming part of an applicable certification scheme (which shall apply when replaced by Annex to the Services Agreement).
8. Supplier's liability for losses arising from breaches of this clause 10 is as set out in Clause 12 (Limitation of Liability).

11. CONFIDENTIALITY

1. Each party undertakes that it shall not at any time use or disclose to any person any Confidential Information of the other party or of any member of the group of companies to which the other party belongs, except as permitted by clause 11.2.
2. Each party may disclose Confidential Information:
    a. to its employees, officers, representatives, contractors, subcontractors or advisers who need to know such information for the purposes of exercising the party's rights or carrying out its obligations under or in connection with the Services Agreement. Each party shall ensure that its employees, officers, representatives, contractors, subcontractors or advisers to whom it discloses the other party's confidential information comply with this clause 11; and
    b. as may be required by law, a court of competent jurisdiction or any governmental or regulatory authority.
3. No party shall use the other party's confidential information for any purpose other than to exercise its rights and perform its obligations under or in connection with the Services Agreement.

12. LIMITATION OF LIABILITY

1. Scope of this clause. References to liability in this clause 12 (Limitation of liability) are subject always to clause 12.3 (liabilities which cannot legally be limited), but otherwise include every kind of liability arising under or in connection with the Services Agreement including but not limited to liability in contract, tort (including negligence), misrepresentation, restitution or otherwise.

2. No limitation of Customer's payment obligations. Nothing in this clause 12 shall limit Customer's payment obligations under the Services Agreement.
3. Liabilities which cannot legally be limited. Nothing in the Services Agreement limits any liability which cannot legally be limited, including but not limited to liability for:
    a. death or personal injury caused by negligence;
    b. fraud or fraudulent misrepresentation; or
    c. breach of the Services Agreement by a proven breach of applicable criminal law.
4. Cap on liability. SUBJECT TO CLAUSE 12.3 (LIABILITIES WHICH CANNOT LEGALLY BE LIMITED), AND TO CLAUSE 12.6, THE LIABILITY OF EACH OF THE PARTIES SHALL NOT EXCEED THE FEES PAID IN THE 12 MONTH PERIOD PRECEDING THE CLAIM OR, WHERE LESS THAN 12 MONTHS HAVE PASSED, THE EQUIVALENT OF 12 MONTHS' WORTH OF FEES, PER CLAIM AND IN AGGREGATE.
5. Specific heads of excluded loss. SUBJECT TO CLAUSE 12.2 (NO LIMITATION OF CUSTOMER'S PAYMENT OBLIGATIONS), CLAUSE 12.3 (LIABILITIES WHICH CANNOT LEGALLY BE LIMITED), THIS CLAUSE 12.5 SPECIFIES THE TYPES OF LOSSES THAT ARE EXCLUDED:
    a. LOSS OF PROFITS;
    b. LOSS OF REVENUES, LOSS OF GOODWILL;
    c. LOSS OF AGREEMENTS, LOSS OF BUSINESS OPPORTUNITY;
    d. LOSS OF BUSINESS;
    e. DEPLETION OF GOODWILL OR SIMILAR LOSSES;
    f. PURE ECONOMIC LOSS; AND
    g. FOR ANY INDIRECT OR CONSEQUENTIAL LOSS, COSTS, DAMAGES, CHARGES OR EXPENSES HOWEVER ARISING.
6. EACH PARTY'S TOTAL LIABILITY TO THE OTHER FOR LOSSES FOR BREACHES OF CLAUSE 9 (INTELLECTUAL PROPERTY RIGHTS), CLAUSE 10 (DATA PROTECTION), CLAUSE 5 (CUSTOMER INDEMNITY) AND CLAUSE 11 (CONFIDENTIALITY), SHALL BE LIMITED TO AND SHALL NOT EXCEED GB£3,000,000.
7. Customer acknowledges that there is a risk that a Service may lead to the loss or corruption of Customer's data affected by the Services, and that the same is an inherent risk of receiving a Service even when performed in accordance with Good Industry Practice. Customer agrees to back up its data prior to delivery of any Service set forth in the Order Form. Except where otherwise provided herein, Supplier will not be liable for any such loss of data.

8. Supplier disclaims and excludes any and all warranties, terms or conditions (not expressly stated in the Services Agreement) as permitted by law, including implied warranties, terms or conditions relating to the acceptable quality and fitness for purpose. Customer is solely responsible for the suitability of the Services chosen.
9. Customer warrants that it has the full capacity and authority to instruct Supplier to deliver the Services and will not hold Supplier liable for any violation of the Computer Misuse Act 1990 or any other local applicable laws, rules or regulations.
10. Except as expressly provided for in the Services Agreement, Customer hereby acknowledges that Services set forth in the Order Form are delivered on an as is basis and Supplier shall only be liable to the extent set forth in the Services Agreement.

13. TERMINATION

1. Either party may immediately terminate the Services Agreement without payment of compensation or other damages caused to the other solely by such termination by giving notice to the other if any one or more of the following occurs:
    a. the other party commits a material breach of any term of the Services Agreement and such breach is irremediable or (if such breach is remediable) fails to remedy that breach within 30 days after being notified in writing to do so;
    b. the other party suspends, or threatens to suspend, payment of its debts or is unable to pay its debts as they fall due or admits inability to pay its debts or (being a company or limited liability partnership) is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986, or (being an individual) is deemed either unable to pay its debts or as having no reasonable prospect of so doing, in either case, within the meaning of section 268 of the Insolvency Act 1986, or (being a partnership) has any partner to whom any of the foregoing apply;
    c. 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 any of 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;

d. 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 (being a company) 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;
e. 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 (being a company);
f. the holder of a qualifying floating charge over the assets of that other party (being a company) has become entitled to appoint or has appointed an administrative receiver;
g. a person becomes entitled to appoint a receiver over all or any of the assets of the other party or a receiver is appointed over all or any of the assets of the other party;
h. 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;
i. 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 13.1(b) to clause 13.1(h) (inclusive); or
j. the other party suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business.

2. For the purposes of clause 13.1(a) material breach means a breach (including an anticipatory breach) that is serious in the widest sense of having a serious effect on the benefit which the terminating party would otherwise derive from a substantial portion of the Services Agreement.
3. Without affecting any other right or remedy available to it, including payment by Customer of all fees due under the Services Agreement, Supplier may terminate the Services Agreement with immediate effect by giving written notice to Customer if Customer is in material breach of any other Supplier Order Form/Services Agreement or fails to pay any amount due under any Services Agreement on the due date for payment and

remains in default more than 30 days after being notified to make such payment.

4. Customer may send express written notice of its intention to terminate the Services Agreement within 30 days of the date it receives 90 days express written notice from Supplier of any material update to the Standard Terms (under clause 17) where that updated term cannot by law or policy, applicable at the time, be accepted by Customer. All fees otherwise due and payable under the Services Agreement must be paid in accordance with the Services Agreement including, without limitation, all fees for any delivered services.

14. CONSEQUENCES OF TERMINATION AND SURVIVAL

1. Consequences of termination or expiry. Except as otherwise provided, the termination or expiry of the Services Agreement shall terminate all licences, access and other rights to the Services and/or Defense.com Platform and Customer shall deliver any Supplier Equipment in its possession to Supplier and destroy all copies of Supplier Confidential Information. Except as otherwise provided, Supplier shall destroy any copies of Customer confidential information. Customer shall immediately pay to Supplier all of Supplier's outstanding unpaid invoices, invoices to be submitted for Services supplied to the date of termination and related interest and, except where Customer has rightfully terminated for Supplier's material breach, Supplier may submit an invoice payable upon receipt in respect of the Services to be supplied but for which no invoice has been submitted.
2. Survival. On termination, where Customer has terminated for Supplier's material breach, or expiry of the Services Agreement, any existing Order Form shall continue until the Services have been completed or, before completion, at Customer's reasonable request. Any provision of the Services Agreement that expressly or by implication is intended to come into or continue in force on or after termination or expiry of the Services Agreement shall remain in full force and effect. Termination or expiry of the Services Agreement shall not affect any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination or expiry, including the right to claim damages in respect of any breach of the Services Agreement which existed at the date of termination or expiry.

15. FORCE MAJEURE

1. Force Majeure Event means any circumstance, except for Customer's payment obligations, not within a party's reasonable control including, without limitation:
    a. acts of God, flood, drought, earthquake or other natural disaster;
    b. epidemic or pandemic or Government mandated lockdowns or other related restrictions;
    c. terrorist or cyber-attack, civil war, civil commotion or riots, war, threat of or preparation for war, armed conflict, imposition of sanctions, embargo, or breaking off of diplomatic relations;
    d. nuclear, chemical or biological contamination or sonic boom;
    e. any law or any action taken by a government or public authority, including without limitation imposing an export or import restriction, quota or prohibition, or failing to grant a necessary licence or consent;
    f. collapse of buildings, fire, explosion or accident;
    g. any labour or trade dispute, strikes, industrial action or lockouts (other than in each case by the party seeking to rely on this clause, or companies in the same group as that party);
    h. non-performance by suppliers or subcontractors (other than by companies in the same group as the party seeking to rely on this clause); and
    i. interruption or failure of a utility service.
2. Provided it has complied with clause 15.4, if a party is prevented, hindered or delayed in or from performing any of its obligations under the Services Agreement by a Force Majeure Event (Affected Party), the Affected Party shall not be in breach of the Services Agreement or otherwise liable for any such failure or delay in the performance of such obligations.
3. The corresponding obligations of the other party will be suspended, and its time for performance of such obligations extended, to the same extent as those of the Affected Party.
4. The Affected Party shall:
    a. as soon as reasonably practicable after the start of the Force Majeure Event but no later than ten days from its start, notify the other party of the Force Majeure Event, the date on which it started, its likely or potential duration, and the effect of the Force Majeure Event on its ability to

perform any of its obligations under the Services Agreement; and

b. use all reasonable endeavours to mitigate the effect of the Force Majeure Event on the performance of its obligations.

5. If the Force Majeure Event prevents, hinders or delays the Affected Party's performance of its obligations for a continuous period of more than six weeks, the party not affected by the Force Majeure Event may terminate the Services Agreement by giving 21 days' written notice to the Affected Party.

16. ASSIGNMENT AND OTHER DEALINGS

1. Customer shall not assign, transfer, mortgage, charge, subcontract, delegate, declare a trust over or deal in any other manner with any of its rights and obligations under the Services Agreement, without prior express written consent from Supplier, such consent not to be unreasonably withheld.
2. Supplier may mortgage, charge, delegate, assign, novate or otherwise transfer any or all its rights under the Services Agreement. Supplier shall not novate or assign its rights and obligations under the Services Agreement to another service party without prior notice to Customer.

17. AMENDMENT

No amendment or variation of the Services Agreement shall be effective without express written consent signed by the parties (or their authorised representatives) except that Supplier may from time to time update the Services Agreement Standard Terms or Services Agreement Service-specific Terms upon 90 days express written notice to Customer upon which Customer may send express written notice of its intent to terminate the Services Agreement as provided for in clause 13.4.

18. WAIVER

1. A waiver of any right or remedy under the Services Agreement or by law is only effective if given expressly in writing and shall not be deemed a waiver of any subsequent right or remedy.
2. A failure or delay by a party to exercise any right or remedy provided under the Services Agreement or by law shall not constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict any further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy provided under the Services Agreement or by law shall

prevent or restrict the further exercise of that or any other right or remedy.

19. RIGHTS AND REMEDIES

The rights and remedies provided under the Services Agreement are in addition to, and not exclusive of, any rights or remedies provided by law.

20. SEVERANCE

1. If any provision or part-provision of the Services Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of the Services Agreement.
2. If any provision or part-provision of the Services Agreement is deemed deleted under clause 20.1 the parties shall negotiate in good faith to agree a replacement provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.

21. ENTIRE AGREEMENT

1. The Services Agreement constitutes the entire agreement between the parties and supersedes and extinguishes all previous agreements, contracts, promises, assurances, warranties, representations and understandings between them, whether written, oral or by conduct, relating to its subject matter.
2. Each party agrees it shall have no remedies in respect of any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in the Services Agreement. Each party agrees it shall have no claim for innocent or negligent misrepresentation or negligent misstatement based on any statement in the Services Agreement.

22. NO PARTNERSHIP OR AGENCY

1. Nothing in the Services Agreement is intended or shall be deemed to establish a partnership or joint venture between any of the parties, constitute any party the agent of another party, or authorise any party to make or enter into any commitments for or on behalf of any other party.
2. Each party confirms it is acting on its own behalf and not for the benefit of any other person.

23. ANTI-BRIBERY AND ANTI-CORRUPTION

Each Party shall, and shall ensure any of its agents, employees, consultants, contractors and subcontractors shall, comply with all applicable laws, statutes, regulation, and codes relating to anti-bribery and anti-corruption including but not limited to the Bribery Act 2010 and shall establish, maintain and enforce its own policies and procedures to ensure compliance.

24. ANTI-SLAVERY AND HUMAN TRAFFICKING

Each Party shall, in performing its obligations under the Services Agreement, comply with all applicable anti-slavery and human trafficking laws, statutes and regulations from time to time in force including the Modern Slavery Act 2015; and each party represents and warrants that it has not been convicted of any offence involving slavery and human trafficking or been the subject of any investigation, inquiry or enforcement proceedings regarding any offence or alleged offence of or in connection with such trafficking.

25. THIRD PARTY RIGHTS

Except as otherwise agreed, the Services Agreement does not give rise to any third-party statutory rights to enforce any of its terms.

26. NOTICES

1. Any notice given to a party under or in connection with the Services Agreement shall be in writing and shall be delivered by e-mail, by hand or by tracked post or courier service at the recipient party's registered office (if a company) or its principal place of business (in any other case).
2. Any notice shall be deemed to have been received:
    a. if by e-mail, at the time of transmission (assuming no failure notification or other indication of non-delivery is received);
    b. if delivered by hand, at the time the notice is left at the proper address; or
    c. if sent tracked and signed-for delivery by national courier, at the time such courier confirms delivery.
3. This clause does not apply to the service of any proceedings or any documents in any legal action or, where applicable, any arbitration or other formal method of dispute resolution.
4. A notice given under the Services Agreement is valid if received.

27. GOVERNING LAW, VENUE AND DISPUTE RESOLUTION

1. The Services Agreement shall be governed and construed in accordance with English law.
2. Any dispute arising under or related to the Services Agreement that is not resolved by good faith discussion among the parties, at their discretion, shall be resolved by binding fast-track London Court of International Arbitration (LCIA) arbitration in London with the exception of an action brought in any court having jurisdiction to enforce terms of an arbitration award under this clause or for injunctive relief or, for Supplier at its discretion, where the sole or primary dispute regards payment by Customer.

28. COUNTERPARTS

The Services Agreement Order Form may be executed and delivered electronically or by hardcopy in any number of counterparts, each of which shall constitute a duplicate original, but all counterparts together constitute the one Services Agreement Order Form. No counterpart shall be effective until each party has executed at least one counterpart.

Services Agreement

Service-Specific Terms

1. A Defense.com Package
2. Consultancy Services
3. Cyber Essentials
4. Incident Response
5. Managed Detection & Response
6. Outsourced Data Protection Officer (DPO)
7. Penetration Testing
8. Virtual Chief Information Security Officer (VCISO)

(incorporated into the Services Agreement Order Form and incorporating the Services Agreement Standard Terms, any Annex and any Order Form Services Addendum, all together the "Services Agreement")

Alphabetical Order

Supplier will provide Customer the following Service(s) as set forth on the Order Form:

1. A DEFENSE.COM PACKAGE

Defense.com is Supplier's SaaS security management solution, the Defense.com Platform, that integrates into any size organisation, providing Customer access to a scalable suite of cyber security tools, each playing a part in protecting Customer's business from new and existing threats and, as a whole, providing Customer's Defense.com Users a Defense.com Licence to access to a 360° view of Customer's security profile 24 hours a day.

A. ASSET PROFILE

Supplier will provide access to Customer to define its digital assets profile which assists in defining the attack surface and allows Supplier to automatically align threats to Customer's unique attack surface. Customer will add assets to ensure the correct threat intelligence feeds align to Customer's environment.

B. BREACH MONITORING

Supplier will provide an automated monitoring solution performing surface web, deep web and dark web scans 24 hours a day for Customer's designated business data which includes Supplier's comprehensive source feeds -- IRC chatrooms, bin sites, data dumps, social sources and dark web sites, to detect sensitive data efficiently.

C. CYBER HEALTH CHECK

Supplier will provide access to an online self-assessment tool that enables Customer to assess its current cyber security and information security posture by answering a series of questions based on modules covering a range of best practice cyber/information security controls, following completion of which Customer will receive an online report of its current status using a RAG (red, amber, green) indication which can be downloaded, and any threats identified will be automatically fed into Customer's Defense.com Threat Dashboard. For each successfully passed question module, Customer may download a pass certificate. Customer may choose which modules to take and can re-take any of the assessment modules at any time.

D. ENDPOINT PROTECTION

Supplier will provide Endpoint Protection software and the SaaS platform to manage the endpoints. Supplier will also provide staff to manage, tune and support the platform. The following are included:

Windows – FileScan; ContentControl; UserControl; Application Backlisting; DataProtection; TrafficScan; AntiPhishing Firewall; BehavioralScan; MailServers (Exchange - only servers); DeviceControl; AntiExploit.

Mac – FileScan; Update Server; and Content Control with TrafficScan + Antiphishing

Linux – FileScan; and Update Server

Customer will install the software to secure endpoints and/or entry points on Customer's end-user devices to prevent file-based malware and detect and block malicious activity through automated vulnerability scanning.

E. MICROSOFT OFFICE 365 MONITORING

Supplier will provide access to the automated Microsoft 365 Monitoring feature which will automatically create threats, escalating the highest risks to Customer and provide remediation advice. Customer will provide support and necessary secure access to Customer's MS Office 365 account with privileges for the Supplier to ingest data and alert on threats identified.

F. PANIC BUTTON

Supplier will provide a 24x7x365 emergency help button which allows Customer to raise potential security incidents with our trained, experienced team. Supplier provides fast-tracked preliminary incident response advice for all types of security events and cyber incidents including, but not limited to, suspected data breaches, ransomware attacks, insider threat, suspicious network activity and known vulnerability exposure. This service is intended to triage potential security incidents and provide practical advice for resolution, but does not include any remediation work from the Supplier.

G. PHISHING SIMULATOR

Supplier will provide access to the Phishing Simulator feature, which enables Customer to send safe phishing emails to test Customer staff's vigilance and identify any weaknesses in their security knowledge. Customer will use the platform to schedule and select the appropriate campaign per team, track results and take remediation steps following the outcome of the test. Customer will setup whitelisting of Supplier IP addresses and email domains as defined in Supplier provided help guides

H. SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Supplier will provide a SaaS based centralised log management to aggregate all log data in a single location and into a common format. Supplier will store log data for 12 months in an archive and provide 90 days of logs for immediate searching. Customer will install with support of Supplier the relevant software and virtual hardware to support the delivery of the service.

I. SECURITY SUPPORT

Provision of a Supplier helpline, including audio and/or messaging, that offers first level response, general guidance and assistance to Customer, within 24 hours of a logged service request (excluding where the response due time falls within a weekend or national holiday), for cyber security questions Supplier deems to be common and frequently asked.

J. THREAT DASHBOARD

Supplier will provide functionality in a single interface that displays threats across all the features provided in Defense.com. Threats are automatically populated by each feature, such as live threat intelligence tailored to Customer. Once threats have been populated, Defense.com provides powerful features to allow Customer to manage each threat and allocate threats to specific individuals for remediation. The platform will assign risk levels and allow the businesses to drill down into specific threat information and understand the business impact. Customer will action threats and perform remediations as identified by the platform or will take action to accept risk or acknowledge threats as false positives.

K. THREAT INTELLIGENCE

Supplier will provide Customer a customised list of cyber threats, continually updated by experts based on the latest intelligence from commercial, opensource and custom-built feeds. Customer will define assets to ensure the correct intelligence is supplied relevant to Customer's environment.

L. THREAT RECON

Supplier will provide access to Threat Recon which presents the attack surface of Customer's business to highlight risks. Threat Recon will automatically perform predefined tests that are used by attackers to test the exposure of the business. These checks include sub-domain detection, port scanning of top 20 ports, network information gathering, SSL validation, potential risk based on site popularity, email spoofing protection checks, block list lookup, security best practices assessment and other checks as offered by Supplier. Customer will provide all relevant internet facing web domains as the scope for the checks.

M. TRAINING VIDEOS & EXAMS

Supplier will provide a range of standard training courses covering varied cyber security, information security and compliance topics. These are delivered through Defense.com with a range of videos and associated exams which, along with built in reporting, allow Customer to track adoption.

N. VULNERABILITY SCANNING

Supplier will provide a platform to allow Customer to run automated Vulnerability Scans of the most common ports with the option to customise to Customer's requirements, to assess systems or applications for known security flaws and weaknesses. Supplier will provide threats that can be managed, allocated, assigned and risks accepted via Defense.com in addition to actionable remediation advice. The service will allow Customer to identify assets that are prone to attacks. Customer will define the scope of the automated scans and take measures to patch or remediate the threats as provided by Supplier's automated process.

2. CONSULTANCY SERVICES

Supplier will remotely provide Customer advice and support covering information security topics, including, without limitation, frameworks such as ISO 27001, NIST, CIS, ISO22301 and General Data Protection Regulation (GDPR) data protection. Where specified, Supplier will assist Customer to work toward improvement of its business performance in terms of operations, management, structure and/or strategy regarding cyber security and/or GDPR compliance. On-site visits may be arranged with Customer in exceptional circumstances.

A. CYBER SECURITY ASSESSMENT

Supplier will provide an experienced Information Security Consultant to assess the current level of information/cyber security in Customer's organisation. This will be based on the NIST CSF and ISO 27001/27002 controls and the output will be a report detailing the level of compliance against each of the requirements along with recommendations on how to achieve compliance.

B. DATA PRIVACY ADVISOR (DPA)

Supplier will provide Customer access to up to 2 hours per month of remote support for queries and questions relating to GDPR and data privacy matters. Customers can contact the DPA service via a centralised mailbox initially and then queries can be dealt with via email, phone or video conferencing.

C. GDPR AUDIT

Supplier will provide an experienced GDPR consultant to audit the current level of compliance to GDPR. The output of the audit will be a report that will outline any non-conformities. During the audit, which will be conducted remotely, Customer will need to provide access to key staff, documentation and evidence to support the audit.

D. GDPR GAP ANALYSIS

Supplier will provide an experienced GDPR consultant to undertake a gap analysis against the requirements of GDPR. The output of the gap analysis will be a report detailing the current

level of compliance to each of the requirements along with a document review (which will include a maximum of 20 GDPR related policies, procedures or documents) with recommendations and an action plan outlining what needs to be done to achieve compliance. During the gap analysis, which will be conducted via a series of online interviews with key stakeholders, Customer will be required to provide documents, e.g., policies and procedures that are currently in place for assessment.

E. GDPR IMPLEMENTATION

Supplier will provide an experienced GDPR consultant to deliver the GDPR implementation project. The service, which will be delivered remotely, will include preparation of all required documentation along with advice and support on how to ensure current processes are compliant. Customer will be required to play an active part in the implementation through interviews and workshops.

F. ISO 27001 GAP ANALYSIS

Supplier will provide an experienced ISO 27001 consultant to undertake a Gap Analysis against, as appropriate, the version of the ISO 27001 standard ISO requested by Customer in accordance with the agreed scope. The output of the gap analysis will be a report detailing the current level of compliance to each of the requirements of ISO 27001 with recommendations on what needs to be done to achieve compliance. During the Gap Analysis, which will be conducted via a series of online interviews with key stakeholders, Customer will be required to provide documents, e.g., policies and procedures that are currently in place for assessment.

G. ISO 27001 IMPLEMENTATION

Supplier will provide an experienced ISO 27001 lead implementer to deliver an ISO 27001 implementation project to enable Customer's readiness for certification by an external UKAS accredited certification body. The implementation service, which will be delivered remotely, will include training of all staff on the Information Security Management System the consultant is implementing and preparation of all required documentation.

Customer will be required to play an active part in the implementation through interviews and workshops.

H. ISO 27001 INTERNAL AUDIT

Supplier will provide an experienced ISO 27001 auditor to conduct an internal audit against the agreed requirements and scope of the Information Security Management System. The output of the internal audit will be a report, written in accordance with the requirements of the ISO 27001 standard that will outline any non-conformities and opportunities for improvement. During the audit, which will be conducted remotely, Customer will need to provide access to key staff, documentation and evidence to support the audit.

I. MANAGED PHISHING CAMPAIGNS

Supplier will perform tailored Phishing simulations (campaigns) to test Customer staff's vigilance and identify any weaknesses in their security knowledge. Supplier will provide a report documenting the results of the Phishing Campaigns through a secure portal. Customer will work closely with Suppliers to agree the scope, requirements of the test, schedule, track results and take remediation steps following the outcome of the test. Customer will provide target employee details including, e.g., their email address, role and full name.

J. PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) CONSULTANCY

Supplier will provide an experienced information security consultant to provide a range of PCI DSS consultancy services to ensure Customer has implemented all the necessary policies, procedures and technical controls to achieve PCI DSS certification. Where available, Customer will be required to provide an asset inventory for systems in scope for PCI along with a network diagram and data flow diagram along with any other relevant supporting policies, procedures and documentation.

K. SERVICE ORGANISATION CONTROL (SOC) 2

Supplier will provide an experienced information security consultant to provide a range of SOC2 consultancy services to assist Customer in the implementation of all necessary policies, procedures and technical controls in preparation for an audit by a Certified Public Accountant (CPA).

L. TRAINING

Supplier will provide a range of standard training courses covering both cyber security awareness and GDPR awareness. These can be delivered through Defense.com with a range of videos and associated exams which, along with built in reporting, allows Customer to track that staff have watched the videos and completed their exams. Other delivery methods include on-site training and virtual training using video conferencing tools. Bespoke training courses covering specific cybersecurity or GDPR topics can also be developed and delivered for Customers in any format, be that video, online training or, where agreed, physically on site. Supplier will provide a copy of any training materials to Customer in pdf format upon completion of the training.

3. CYBER ESSENTIALS

Supplier will assist Customer to achieve certification under the NCSC Cyber Essentials scheme. Support is provided in line with the level of service Customer has contracted for as per the following:

Feature	Essentials	Essentials Premium	Ess
Cyber Essentials certification	Included	Included	Included
Cyber Essentials Plus certification			Included
Up to 25k FREE cyber insurance*	Included	Included	Included
Free additional cyber protection tools (i)	Included	Included	Included
Tailored policy documents		Included	
Remote support (ii)	2h included	4h included	4h included
Free retest	1 free retest	1 free retest	1 free retest

Supplier in addition will provide:

i. Additional cyber protection tools as specified on the Order Form such as: vulnerability scanning, endpoint protection, online training and exams and Asset Profile.
ii. emote support via telephone, email or video conferencing. Additional support time required is available at our standard rate.

*Cyber Insurance:

Free cyber insurance, provided by a third party insurer, is provided to UK companies as part of the scheme if the basic certification covers the entire organisation.

Customer acknowledges that the Cyber Essentials scheme is intended to reflect that the certificated organisation has established the cyber security profile set out in the Cyber Essentials scheme documents only and that receipt of a scheme certificate does not indicate or certify that the certificate holder is free from cyber security vulnerabilities. Customer acknowledges that Supplier has not warranted or represented the Cyber Essentials scheme or certification under the Cyber Essentials scheme as conferring any additional benefit to Customer.

C. CYBER ESSENTIALS (EXCLUDING CYBER ESSENTIALS PLUS)

After purchasing Cyber Essentials, Customer will be required to confirm via email when they are ready to complete their assessment. The Cyber Essentials team will send an email after initial purchase, asking to be informed when Customer is ready to proceed. Customer will not be given access to complete their assessment until a response is received.

Customer shall complete and submit the self-assessment form within a month of being added to the portal.

Customer shall comply with the Cyber Essentials scheme documentation and all reasonable directions made to Customer by the Authority, a Cyber Essentials Partner or a certification body.

Subject to Customer's completion of a Cyber essentials self-assessment (the "Questionnaire"), Supplier will assess the Customer-completed Questionnaire against the Cyber Essentials Scheme criteria.

The Questionnaire account will remain open and accessible for six (6) months. If Customer has not submitted the Questionnaire within 6 months, the assessment will expire and no refund will be permitted. If Customer wishes to complete the Questionnaire

after expiration, it will be required to order Cyber Essentials again.

If the completed Questionnaire assessment meets the Cyber Essentials scheme criteria (which Supplier shall assess in accordance with the IASME marking scheme) Supplier will notify Customer and, subject to Customer meeting its obligations, Supplier will arrange for the issue of a IASME Certificate to Customer.

If a certification only service has been purchased by Customer, no support will be provided by Supplier other than assistance gaining access to the Questionnaire.

If Customer has not submitted its application after a month of being added to the portal, reminders will be sent to Customer as follows:

- After 4 weeks of inactivity – one reminder email will be sent to the main contact on the application.
- After another 2 weeks a second reminder will be sent if Customer has still not submitted its application.
- After another 2 weeks a third reminder will be sent if Customer has still not submitted its application.
- After another 2 weeks a fourth and final reminder will be sent if Customer has still not submitted its application.

If all the above reminders do not result in a reply with either an offered date or a submission, the customer will be invoiced either at the point where their account expires (6 months after the questionnaire account being added) or when their contract ends, whichever is sooner.

Where Customer's order has not been completed within 12 months from the date it was placed, the assessment will be marked as a 'fail' and Customer will be invoiced.

Cancellation of orders is not possible due to the systems and third parties involved in providing the service. Therefore, incomplete applications will be marked as a 'fail' and Customer will be invoiced.

D. CYBER ESSENTIALS PLUS:

Customer must achieve an additional cyber essential level within 90 days of certifying against Cyber Essentials (excluding Plus). Any free retest offerings must be used within the 90-day deadline for completing Cyber Essentials Plus.

If Customer is unable to pass within that time through no fault of Supplier, the application will be marked as a 'fail'.

Where Customer fails the Cyber Essentials Plus test, Customer will have 30 days to remediate any issues found and get a retest (within the 90 days).

Where Customer refuses or fails to provide the access required to conduct the test, the test will be marked as a 'fail'.

If Customer wishes to move their assessment date, Customer must provide Supplier with at least 48 hours' notice. Failure to provide the requisite notice to Supplier will incur cancellation charges in line with the Services Agreement Standard Terms.

4. INCIDENT RESPONSE

Supplier will provide Customer assistance within three hours via Supplier's SOC hotline which is available 24x7x365. The emergency request will consist of an initial assessment and triage via phone to discover and confirm the nature and impact of the incident within Customer's environment, including the collection and analysis of all relevant information, and to provide advice based on the nature of the incident. Customer will provide all necessary resources and information to ensure the success of the service. If more detailed analysis is required or the incident has been confirmed as a data breach the service will provide additional support to investigate the extent of the incident which may include forensic analysis supported onsite (Digital Forensics) where required at an additional cost as defined in the Services Agreement Standard Terms. Digital Forensics support will be charged, as required, at a day rate of ~£1,500.00 as updated by Suppler from time to time.

A. Customer shall provide and coordinate Supplier's access to the systems to be investigated. Before any system access is granted, Customer shall inform Supplier in writing and in advance of any security and access standards or requirements that may change.

B. During an assessment, the configuration of Customer's network will be kept as stable as possible (i.e., no new systems or configuration changes). If changes are required, Customer shall inform Supplier, and a mutually acceptable testing schedule shall be agreed upon.
C. During the initial notification call, Customer shall provide Supplier with information below to create an incident ticket. Customer shall appoint an authorised contact person for every incident raised. The appointed contact person shall be preregistered with Supplier.

   Customer Name

   i. Locations affected by the incident
   ii. Priority of the incident
   iii. Information on how the incident was identified

   Contact Name

   iv. Contact Phone Number
   v. Details of incident
   vi. Information on when the incident was first identified

   Note: Should Customer consider the nature of the incident to preclude the support desk being provided with these details, Customer contact may simply state that the incident is a 'flash priority' at which point Supplier support personnel will request no further details and will immediately initiate the response procedures.

D. It is also the responsibility of Customer to provide details of the priority classification for discussion prior to rollout of the services. Further to this, it is considered Customer's responsibility to make the following information available and the processes followed. Supplier will work closely with Customer (as a separate engagement) to ensure that all responsibilities can be met.
E. Customer shall maintain accurate network diagrams and make these diagrams available to Supplier as required.
F. Customer shall maintain accurate process maps and diagrams, detailing the systems involved with the transmission, storage, or processing of sensitive information.
G. Customer shall provide an updated list (per incident) of personnel with which the aspects of the incident may be openly

discussed. All other personnel will simply be directed toward their own management for information.

H. Customer shall provide contact information for senior personnel related to affected departments or systems to be contacted for further information (see previous point).

5. MANAGED DETECTION & RESPONSE

Supplier will provide a SaaS based security information and event management platform to deliver real-time analysis of potential cybersecurity threats. Supplier's security analysts will analyse Customer logs 24x7x365 to identify security threats and raise events to Customer for investigation. Customer will install, with the support of Supplier, relevant software and virtual hardware to support the delivery of the Service.

A. DEFINITIONS

The following additional definitions shall apply to this Service:

"APT" or "Advance Persistent Threat" means a set of stealthy and continuous computer hacking processes.

"Attack" means the inflow of malicious or illegitimate call requests to an infrastructure or web platform for malicious intent. The purpose of this is to gain access or to deliver disruption to the infrastructure.

"Critical" means the classification by Supplier of a Security Event as defined in the Managed Detection & Response Service Level Agreement (MDR SLA) that will receive the highest level of response from Supplier's designated trained security professionals.

"Incident Response Plan" means the overarching framework for both parties' efficient and professional reactions during a security incident.

"Non-Critical" means a Security Event as defined in the MDR SLA that does not require immediate attention because it is deemed not to be critical.

"Runbook" means a routine compilation of procedures and operations which designated employees will use as a reference.

"Security Event" means a change in the everyday operations of a network or information technology service, which indicates that a security policy may have been violated or a security safeguard may have failed.

"Security Incident" means a situation where an adverse impact has resulted from a Security Event.

"SIEM" means software products and services combining security information management (SIM) and security event management (SEM) that provide real-time analysis of security alerts generated by network hardware and software applications.

"Threat Investigation" means any actions taken by Supplier to validate a Security Event as a real threat and to rule out the possibility of it being a false alert.

"Threat Signatures" means any information provided by Vendors to help identify any threats that could impact Customer's network or infrastructure.

"Vendors" means third parties who provide Supplier with infrastructure, products, intelligence or expertise to allow us to provide the Services, including but not limited to dedicated hardware appliances, Threat Signatures, and vulnerability scanning services.

"Zero-day" means an attack that exploits a previously unknown vulnerability in a computer application or operating system, one that developers have not had time to address and patch.

B. SUPPLIER OBLIGATIONS

Supplier will provide the following in accordance with the Order Form, the MDR SLA and Runbooks.

Active monitoring of all systems in scope for Security Event using a threat intelligence SIEM module.

Correlate various logs to identify any Security Events that may carry a potential threat.

Interpretation of logs and audit trail and focus on threats that matter most to Customer.

Incident investigation from triggered alerts and abnormal behaviour in accordance with a well-defined and agreed Runbook.

Customer notification and incident reporting in accordance with the agreed incident response plan.

Provide recommendations for dealing with incidents.

Ongoing management and maintenance of the threat (SIEM) appliances: installation, migration and configuration of the SIEM hardware or software.

All configuration files will be kept and backed-up for a minimum of 30 days with daily restore points covering one week, unless an alternative period is formally requested by Customer and agreed by Supplier.

All logs will be kept and backed-up for a minimum period of 30 days, with immediate access and 1 year in archive.

Incident reports will be generated within 24 hours following any critical Security Event as soon as the investigation has been completed. Upon request, Supplier will provide incident reports for any critical Security Events that have occurred.

Access to an online portal which will contain up-to-date incident reports and change control information.

C. CUSTOMER OBLIGATIONS

Customer agrees to perform the obligations and that Supplier's ability to perform its obligations and its liability are dependent on Customer's compliance with the following:

Customer is required to make appropriate staff available to help Supplier with the following items (if applicable):

i. Runbooks
ii. Incident Response Plan
iii. Any other documents or procedures required to provide the Services.
iv. Any infrastructure or platform used to provide the Services
v. Any other procedures required to provide the Services

In the case of a Security Event occurring, Customer agrees to work in line with agreed Runbooks.

Customer agrees and understands that the effectiveness of the Services depends on the collaboration during the on-boarding phase that will define and assess the processes, escalation points and on-going communication channels.

Customer must inform Supplier of any changes that could affect any individual Runbook or the Incident Response Plan. This also includes the escalation procedures, availability and contact details of personnel, reliability, performance and any other security or compliance related requirements.

D. SUPPLIER MDR SLA

Supplier will work in line with the agreed Runbooks.

Supplier will monitor all key components used in the delivery of the Services 24x7x365.

In the event of any issues arising, Supplier will work to identify and resolve any threats or issues as quickly as possible.

Supplier will provide technical staff 24x7x365 to support the Services provided and to assist Customer with any issues that may arise. A 24-hour telephone number will be available for Customers. Email support will also be provided but should not be used for emergencies.

If a Critical event occurs, Supplier will perform an initial Threat Investigation and then notify Customer within 30 minutes of the Security Event if it has been deemed by Supplier to have become a Critical event.

If a Security Event occurs of a Non-Critical nature, Supplier will take actions in line with the agreed Runbook.

If a Security Event occurs Supplier will first carry out a Threat Investigation and will then respond to Customer within the timeframes listed in the table below.

For any Security Event which Supplier deems to be Critical prior to the Threat Investigation being completed, Supplier will contact and regularly update Customer.

The Security Event severity is typically set via the stage at which the event comes in the attack kill chain. The further along this process the more severe the event.

SEVERITY LEVEL	EXAMPLE
Critical	Command and Control communication established / outbound connection known bad actor address
High	Brute-force activity against externally facing systems with legitimate acc
Medium	Infrastructure or system version Information disclosure
Low	Administrator account lockout
Informational	Reconnaissance such as Port Scanning

EXCLUSIONS

Supplier will not be liable under the following conditions:

i. Where scheduled maintenance was being carried out;
ii. Where there has been any act or omission of Customer (or its Representatives) in breach of the Services Agreement;
iii. For any security breaches caused by any Customer changes of which Supplier was not made aware;
iv. For any security breaches where Supplier takes an action requested by Customer which has not been agreed or tested as part of creating the relevant Runbook;
v. Where Threat Signatures were not available by the Vendors to allow Supplier to identify a threat including but not limited to Zero-day Attacks and APTs.

6. OUTSOURCED DATA PROTECTION OFFICER (DPO)

A managed service where Customer can purchase a number of days (smallest amount is 0.5 days) per month for DPO services. Where Customer does not use the total amount of time in any given month, that time may be carried over to the subsequent month (but not longer).

Supplier will provide virtual consultation to Customer, information, advice and other related services, in accordance with the DPO Service Levels below, to ensure that Customer processes the personal data of its staff, customers, service providers or any other individuals (also

referred to as data subjects) in compliance with Applicable Data Protection Laws and best practice.

A. SUPPLIER OBLIGATIONS

Supplier will:

Act as the Data Protection Officer (DPO) for Customer in accordance with Applicable Data Protection Laws;

Facilitate Customer compliance with the UK/EU GDPR and other applicable data protection legislation by ensuring effective systems and controls are in place to enable Customer to comply with their legal obligations;

Act as Customer's intermediary between relevant stakeholders, including supervisory authorities, data subjects, and business units;

Report notifiable data breaches identified and notified to Supplier by Customer to the Information Commissioner's Office (ICO) and any relevant supervisory authority at the end of any statutorily required notice period where the requisite notice has not been sent earlier either by Customer or Supplier at Customer's instruction; and

Inform and advise Customer's senior management (where appointed to do so) in accordance with Supplier's position as DPO of Customer.

B. CUSTOMER OBLIGATIONS

Customer will ensure compliance with all Applicable Data Protection Laws and in particular Customer will:

Report all notifiable and potential data breaches to Customer assigned DPO dposupport@bulletproof.co.uk as soon as Customer becomes aware of the breach;

Submit details of data breach(es) to Supplier for reporting to the ICO and any relevant supervisory authority without undue delay; and

Where Customer fails to comply with reporting obligations above, Supplier shall not be liable and Customer will indemnify Supplier for any penalties imposed by the ICO, any relevant supervisory authority or any third-party claims, because of failure and or delay in reporting notifiable breaches.

C. DPO SERVICE LEVELS

Priority levels will be addressed in line with the following Service Levels.

Type	Respo
Critical	within 1 Hour
Urgent	within 4 Hours
Non-urgent	by the end of the Next Business Day

All Service Levels apply only from 9:00am to 5:30pm GMT Monday to Friday excluding UK bank holidays ("Working Hours"). All DPO Service requests must originate with an email sent to the allocated DPO and copied to dposupport@bulletproof.co.uk and the subject line must contain the priority in accordance with the following:

i. "Critical" a scenario which will have serious immediate impact on the protection of personal data
ii. "Urgent" for advice on GDPR/data protection topics that are subject to time constraints
iii. "Non-urgent"for advice and guidance on GDPR/data protection issues and longer term projects that do affect Customer's operations.

7. PENETRATION TESTING

Supplier will perform penetration testing that evaluates Customer systems to validate and exploit known vulnerabilities by assessing critical external and/or internal assets and/or APIs and/or web applications and /or mobile applications and/or cloud infrastructure and/or wireless infrastructure using experienced penetration testers to determine if Customer's organisation is susceptible to attacks. Supplier will provide a report in both online and downloadable versions within 5 working days of completion of a test.

A. DEFINITIONS:

"Late Availability Test" where Customer contacts Supplier to conduct Penetration Tests with five working days or less notice.

"Red Team Penetration Test" means the onsite presence of Supplier who will test the System as described in a scope Annex made by Supplier to Customer.

"Test Start Time" means the provisional or definitive date and time listed in the Order Form (or otherwise later expressly agreed by the parties in writing) that determines when the Services will commence.

B. CUSTOMER OBLIGATIONS:

To submit, by upload into the Defense.com platform (Penetration Testing dashboard), any necessary further scope details at least five working days prior to the start of the Penetration Tests for efficient scheduling of necessary resources and time.

Where Customer fails to submit the necessary scope details, Supplier shall reschedule the Penetration Test and Customer shall be liable for any charges.

Customer and Supplier will agree dates promptly after the Commencement Date or as set forth in the Order Form for Supplier to deliver the Services within 12 months of the execution of the Order Form and, where Customer fails to agree dates for the Services through no fault of the Supplier, Customer will forfeit their right to the Services for the relevant 12-month period and, for the avoidance of doubt, no refund or waiver of Fees or related costs, all owed upon execution of the Order Form, will be issued by Supplier.

Where Customer requests a Late Availability Test and fails to timely provide Supplier with the necessary information to commence the Penetration Test, Supplier shall not be obliged to carry out the relevant Services and Customer will not be entitled to any refunds or waiver of Fees or related costs.

Customer acknowledges that the Service will be provided remotely unless explicitly requested and agreed otherwise. If onsite access is required to facilitate testing, Supplier will provide the option of customer present equipment (CPE) to

facilitate remote testing from Supplier's secure remote location. In person tests may be provided upon request by Customer or Supplier, subject to approval by Supplier.

Customer acknowledges that a Penetration Test is a snapshot in time and that it is limited to the actions set out on the Order Form (which actions may be agreed in an incorporated scope Annex document).

Customer shall comply with any rules imposed by any third party whose content or services are accessed via the Services.

Customer shall inform Supplier forthwith if any of the Services are subject to interference or malfunction.

Customer, prior to Penetration Tests, must proactively and appropriately backup all critical data from its Systems that will form part of the Penetration Tests.

Where Customer engages Supplier to provide a Red Team Penetration Test, Customer further represents and warrants to Supplier that Customer: a) has the necessary authority to instruct Supplier to provide the Red Team Penetration Test; and b) shall sign a letter of authority (duly signed by an authorised member of the executive board or equivalent) in the eventuality that Supplier requires it.

8. VIRTUAL CHIEF INFORMATION SECURITY OFFICER (VCISO)

Supplier will provide a remote managed service that includes an experienced Information Security Consultant to build and implement information security strategy for Customers. The service may require an initial health check to establish the current security posture of Customer's organisation and enable Supplier's Consultant to build a strategy. This Service can also provide support to manage existing security frameworks such as Cyber Essentials and ISO 27001. On-site visits may be arranged, where agreed, with Customer in exceptional circumstances.

A. SUPPLIER OBLIGATIONS

Supplier will provide regular updates to Customer where reasonably requested;

Supplier will provide regular (at least monthly, at Supplier's discretion) updates on the progress of the implementation of the agreed security strategy;

Supplier will only amend any agreed strategy with the written agreement of Customer; and

Supplier will work with third party suppliers of Customer where reasonably requested (e.g., outsourced IT providers).

B. CUSTOMER OBLIGATIONS

Customer will notify Supplier's designated VCISO of changes to Customer's business including, interpreted broadly:

i. Structural/organisation changes e.g., acquisitions, sales;
ii. Critical role and responsibility changes;
iii. Key Customer supplier changes that may impact on information security;
iv. New Customer supplier onboarding that may impact information security;
v. New software/solutions/hardware/cloud services that are planned; and
vi. Key personnel changes.

Customer will notify the VCISO of any security incidents or data breaches of which it becomes aware.

Customer will notify VCISO of any Customer regulatory, legislative and/or contractual requirements.

Customer will, when raising a request for assistance from its VCISO, ensure that vciso@bulletproof.co.uk is copied on all messages.