Cyberis

G-CLOUD 14

Terms and Conditions

Cyberis Limited
Unit E, The Courtyard, Tewkesbury Business Park, Tewkesbury, Gloucestershire, GL20 8GD
T: +44 1684 353514 | E: info@cyberis.com | W: cyberis.com

Cyberis Standard Terms

These are the terms on which Cyberis Limited (**Cyberis**) do business. They do not affect the Client's statutory rights. They are designed to set out clearly Cyberis' and the Client's rights and responsibilities.

The Cyberis Standard Terms include the **CVA Services Terms** (when CVA Services are purchased by the Client) and the **CSIR Retainer Services Terms** (when CSIR Retainer Services are purchased by the Client).

GENERAL TERMS

1. Definitions and Interpretation

1.1. The following words and phrases have the following meanings in this Agreement:

WORD OR PHRASE	DEFINITION
Affiliate:	means any legal entities that Control, are Controlled by, or are under common Control with, the referenced Party from time to time.
Agreement:	means collectively these Cyberis Standard Terms; the CVA Services Terms (when CVA Services are purchased by the Client); the CSIR Retainer Services Terms (when CSIR Retainer Services are purchased by the Client); all Statements of Work; and all Changes.
Applicable Law:	means all of the following to the extent that they apply to the subject matter of this Agreement: • any statute or regulation, in force from time to time; • any court order, judgment or decree binding on the applicable Party; and • any applicable direction, statement of practice, policy, rule or order that is set out by a regulatory authority.
Change:	means each contractually binding amendment to this Agreement that has been duly executed by both Parties.
Charges:	means the charges payable by the Client to Cyberis for the Services (as specified in the applicable Proposal and Statement(s) of Work) in Pounds Sterling (GBP) unless stated otherwise.
Claims:	means claims or proceedings made, brought or threatened by any person against the applicable Party.
Clause:	means a clause of these Cyberis Standard Terms.
Client:	means the corporate entity that has executed this Agreement to procure Services from Cyberis.
Client Personnel:	means all employees, staff, workers, agents and consultants of the Client or any Client sub-contractor that receives or benefits from the Services.
Client Property:	means computer systems; servers; technology infrastructures; telecommunications or electronic communications systems and associated communications; confidential information; data (including Client's Personal Data, employee identification, authentication or credential data, user details and other sensitive information); assets; devices; intellectual property; and/or physical premises, that are used by the Client, its employees, clients, or suppliers, whether owned or otherwise controlled by the Client or owned by a third party.
Confidential Information:	means information in whatever form including without limitation:

WORD OR PHRASE	DEFINITION
	• information in written, oral, visual or electronic form or on any magnetic or optical disk or memory relating to the business, customers, products, affairs and finances of the applicable Party; • trade secrets including, without limitation, technical data and know-how relating to the business of such Party or any of its or their suppliers, customers, agents, distributors, shareholders, management or business contacts; and • information that the Party creates, develops, receives or obtains in connection with the Services, whether or not such information is marked or designated confidential; but excluding information that: (a) is publicly available (other than through a breach of Clause 11 (*Confidentiality*); (b) was received from a third party who did not acquire it in confidence; or (c) is developed without any breach of this Agreement.
Contract Acceptance Form:	means Cyberis' online form which may be used to execute the Agreement in the absence of a Purchase Order.
Control:	has the meaning set out in Section 1124 of the UK Income and Corporation Taxes Act 2010 and **Controlled** is construed accordingly.
CSIR Retainer Services Terms:	means the additional Cyberis terms and conditions that apply when the Client purchases CSIR Retainer Services.
CVA Services Terms:	means the additional Cyberis terms and conditions that apply when the Client purchases CVA Services.
Cyberis Personnel:	means all employees, staff, workers, agents and consultants of Cyberis or any Cyberis sub-contractor engaged in the performance of the Services.
Data Controller, Data Processor, Data Subject, Personal Data,	shall have the meanings attributed under the applicable Data Protection Laws (and the Client consents to Microsoft Corporation, Amazon Web Services EMEA SARL and Egress Software Technologies Limited as Sub Processors).

WORD OR PHRASE	DEFINITION
Process and Processing:	
Data Protection Laws:	all laws (and regulations having the force of law) relating to the protection of Personal Data, including: • the UK Data Protection Act 2018 (DPA) and the EU General Data Protection Regulation 2016/679 (**GDPR**) as implemented in the laws of the UK General Data Protection Regulation (**UK GDPR**); • the Regulation of Investigatory Powers Act 2000 (**RIPA**); • the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000; • the Privacy and Electronic Communications Directive 2002/58/EC; and • the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426); in each case as may be amended or replaced and together with the equivalent legislation of any other applicable jurisdiction and all other applicable law, regulations and codes of conduct in any relevant jurisdiction relating to the processing of Personal Data and privacy including the guidance and codes of practice issued by a relevant Regulatory Authority.
Force Majeure:	means circumstances beyond the reasonable control of the Party seeking to rely on it as a reason for non-performance including but not limited to any of the following: • war, strike, riot, crime, government travel restrictions, acts of God, or shortages of resources; • legal prohibition, passing of a statute, decree, regulation or order that impedes the Services; or • if Cyberis resources are unable to obtain (or are delayed in obtaining) visas prior to performing work in Client's country.
Intellectual Property:	means inventions, discoveries, ideas, concepts, methods, manufacturing processes, unique compositions, code, executables, works of authorship, know-how, designs, mask works, and materials (including any derivatives of the preceding

WORD OR PHRASE	DEFINITION
	items); whether or not patentable, copyrightable or subject to mask work rights or other forms of protection.
IPR:	means all rights of ownership or use over Intellectual Property including patents, utility models, rights to inventions, copyright and neighbouring and related rights, moral rights, trademarks and service marks, business names and domain names, rights in get-up, goodwill and the right to sue for passing off, rights in designs, rights in computer software, 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.
Liability:	means liability arising out of or in connection with this Agreement, whether in contract; tort; misrepresentation; restitution; under statute or otherwise including any liability under an indemnity contained in this Agreement and/or arising from a breach of, failure to perform, or delay in performing any of a Party's obligations under this Agreement howsoever caused including if by negligence.
Parties:	means Cyberis Limited and the Client (and **Party** means either of them).
Person Day:	means a period of 7.5 Working Hours.
Proposal:	means a proposal prepared by Cyberis specifying the Services that the Client purchases under this Agreement.
Section:	means a section of the applicable Proposal or Statement of Work.
Services:	means the services to be delivered by Cyberis to the Client under this Agreement (as specified in detail in each Proposal and each Statement of Work and which will include the CVA Services when purchased by the Client and the CSIR Retainer Services when purchased by the Client).
Services Commencement Date:	means the date specified as such in each Proposal and each Statement of Work or (where not specified) a mutually agreed date upon which Cyberis will start to provide the Services.
Services Specifications:	means the specification(s) for the Services as detailed in each applicable Proposal or each Statement of Work.
Statement of Work:	means a contractually binding supplement to this Agreement that specifies additional or ad hoc Services that are not otherwise specified in a Proposal.
Working Day:	means any day other than a Saturday, Sunday or public holiday in England.
Working Hours:	means, unless otherwise agreed, 09.00 to 17.30 (UK time zone) on each Working Day.
Work Product:	means any reports, documents, work product or other materials created by Cyberis for the Client arising from the Services.

1.2. Headings are for ease of reference and do not affect the interpretation of this Agreement.

1.3. References to a person include any individual, body corporate, partnership, government authority, agency or department, state or any other entity (in each case whether or not having separate legal personality).

1.4. Any phrases following the words **include**, **in particular** or any similar expressions shall be construed without limitation and accordingly shall not limit the meaning of the words preceding them.

1.5. An obligation on a Party to procure or make sure the performance or standing of another person shall be construed as a primary obligation of that Party.

1.6. A reference to a statute or statutory provision is a reference to it as amended or re-enacted. A reference to a statute or statutory provision includes all subordinate legislation made under that statute or statutory provision.

2. Status and Formation of this Agreement

2.1. This Agreement shall:

2.1.1. apply to all Services, Statements of Work and all Changes executed by both Parties from time to time; and

2.1.2. prevail over any terms or conditions contained in, or referred to in, the Client's purchase order, confirmation of order, specification, or any other document or which are implied by trade, custom, practice or course of dealing.

2.2. This Agreement constitutes a binding contract on the earliest to occur of:

2.2.1. the Client returning the Contract Acceptance Form (duly executed);

2.2.2. the Client notifying Cyberis by email (or otherwise) that the Proposal has been accepted and Cyberis should commence providing Services; or

2.2.3. the Client issuing a purchase order for the Services based on the Proposal.

3. Supply of Services

3.1. Cyberis shall perform Services to meet the Services Specifications and, in accordance with the timetable as set out in the applicable Statement of Work or (where not specified in the Statement of Work) the Parties shall mutually agree a Services Commencement Date or timetable to perform the Services.

3.2. Where Cyberis is unable to perform the Services on the dates specified in the Statement of Work and/or previously agreed dates and times, Cyberis shall use reasonable endeavours to inform the Client prior to the scheduled dates and to arrange alternative mutually convenient dates as close as is reasonably practicable to the original dates.

3.3. The Client shall be deemed to have accepted the Services when the Services in all material ways comply with the applicable Services Specifications.

3.4. Cyberis shall:

3.4.1. perform Services with the levels of care, skill and diligence that would be applied by any reasonable and professional UK-based supplier of similar services;

3.4.2. use sufficient number of Cyberis Personnel who are suitably skilled to perform the Services;

3.4.3. ensure that the Services conform with the Client's reasonable written additional instructions, unless the instructions represent material changes to, or contradict or expand the scope of, the Services (and therefore subject to a formal Change which may potentially include a Charges adjustment – if Cyberis incurs additional costs in complying with those additional instructions);

3.4.4. ensure that the Services do not knowingly or negligently infringe the IPR of any third party;

3.4.5. provide all equipment, tools and vehicles and other items required for Cyberis to provide the Services;

3.4.6. obtain, and at all times maintain, all licences and consents required for Cyberis to provide the Services;

3.4.7. ensure that Cyberis Personnel are insured appropriately whilst working on the Client's premises; and

3.4.8. comply with all applicable laws, regulations, regulatory policies, guidelines or industry codes which apply to the provision of the Services in the United Kingdom.

3.5. Cyberis does not guarantee the performance of any Client software or hardware even if Cyberis supports such hardware or software as part of the Services.

3.6. Cyberis shall not be responsible for any failures in Client or Cyberis hardware or software due to manufacturer design or failure.

3.7. Cyberis Personnel operating at Client premises shall observe all reasonable health and safety rules and regulations and any other reasonable security requirements that apply at those Client premises and that have been notified in advance to Cyberis by the Client in writing.

3.8. Cyberis may substitute Cyberis Personnel at short notice, giving the Client as much notice as possible.

3.9. The Services are provided for the Client and not for the benefit of any third parties. If a third party includes Cyberis on any lawsuit or similar Claim related to a Client security incident for which Cyberis provided Services, the Client will defend and hold harmless Cyberis against such claims, including any related costs and liabilities.

3.10. Cyberis may sub-contract the provision of all or part of the Services to any person or party, but such sub-contracting shall not relieve Cyberis from its obligations under this Agreement.

4. Changes

4.1. If either Party wishes to change all or any part of the Services, that Party will provide full written particulars of such proposed changes to the other Party (**Proposed Change**). The Parties shall promptly in good faith review and discuss the Proposed Change and, if agreed, shall execute a Change to amend the Agreement accordingly.

5. Client Specific Obligations

5.1. The Client shall provide Cyberis with accurate, complete and timely information and/or instructions as required to enable Cyberis to provide the Services, and promptly notify Cyberis of any changes to circumstances which could render any information previously provided to be inaccurate which may have a bearing on the Services. Cyberis does not bear any liability for inaccuracies, errors, losses, damages, failures, any missed timelines or problems which arise as a result of the Client not providing Cyberis with accurate, complete and timely information and/or instructions.

5.2. The Client shall, in a timely and efficient manner:

5.2.1. allow Cyberis access to the Client Property in a suitable operational state and in accordance with Applicable Law to enable Cyberis to carry out safe and efficient provision of the Services without delay and/or interruption;

5.2.2. provide all the Client pre-requisites as specified in an applicable Proposal or Statement of Work (as required both before and after the Services Commencement Date) including providing:

(a) cooperation of sufficient suitably authorised and qualified members of the Client Personnel as may be reasonably requested by Cyberis; and

(b) access to accounts, credentials, access to systems, documentation, data and/or information as may be reasonably requested by Cyberis;

5.2.3. provide and maintain all networks and communications media that are not specifically identified as a Cyberis obligation, and diagnose/resolve any technical issues encountered by Cyberis in the Client Environment and Facilities;

5.2.4. procure any applicable consents and authorisations that may be necessary under law or Client's agreements with third parties for Cyberis to perform the Services (onsite or remotely, as applicable);

5.2.5. create regular data backups of all data stored on all Client systems, networks and devices in such a manner as to minimise any potential data loss or corruption that could be caused by the Services;

5.2.6. notify Cyberis of any applicable export control requirements related to Client Property and obtaining any required licenses with respect to the export of any such Client Property in connection with the Services;

5.2.7. be responsible for determining whether to use or refrain from using any recommendation that may be made by Cyberis; and

5.2.8. where applicable, provide support for Cyberis to obtain any required visa and/or travel authorisations to provide the Services.

5.3. The Client shall not instruct Cyberis to perform Services which cause Cyberis to be in breach of any law or regulation in the UK or any other applicable jurisdiction.

5.4. If the Services include technical security assessments, penetration testing, 'hacking' of the Client's information technology infrastructure or other Client asset and/or any activities that would normally be categorised as an offence under Applicable Law (including, for example, the UK Computer Misuse Act 1990):

5.4.1. the Client hereby consents to Cyberis carrying out such activities and grants to Cyberis authority to carry out such activities;

5.4.2. the Client shall procure any applicable consents and authorisations that may be necessary under Applicable Law or the Client's agreements with third parties for Cyberis to perform the Services (onsite or remotely, as applicable);

5.4.3. the Client shall take all actions necessary to grant Cyberis access to all Client Property related to the Services, including without limitation, if applicable, consent to connect to the Client's computer network, install software and/or hardware, and collect and analyse data; and

5.4.4. the Client shall be solely responsible for providing instructions or obtaining any necessary consents for Cyberis to provide the Services in compliance with Applicable Law, including without limitation, any laws relating to network integrity or security or to data privacy or data protection. If the Client fails to obtain any such consents, the Client shall be solely and fully responsible for any related claims or liabilities (notwithstanding any contrary terms in this Agreement).

6. Security, Ransomware and Virus Protection

6.1. Without limiting Clause 10 (*Liability and Insurance)*, Cyberis does not accept liability in any form for direct or indirect loss, impact to business or loss of service as a result of any third party security breach, ransomware, virus attack or other electronic means of compromise under any circumstances.

6.2. Cyberis does not warrant or guarantee protection against third party malicious behaviour, nor does it guarantee the availability or performance of security appliances or software as part of the Services.

6.3. If Cyberis identifies areas of potential risk outside the scope of the Services, Cyberis shall use reasonable endeavours to inform the Client of the issue identified for review and relevant remedial advice. Any such remediation advice would be contracted as additional Services on a case-by-case basis.

6.4. Cyberis may become aware of issues such as data breaches, network intrusions, or the presence of malware, and that such issues may give rise to regulatory reporting obligations which the Client may be subject to in one of more territories in which the Client operates. The Client will remain solely responsible for all such reporting requirements and Cyberis shall not have an obligation to report unless applicable legal or regulatory obligations require Cyberis to do so.

7. Personal Data Protection

7.1. Each Party shall comply with their obligations under the Data Protection Laws which arise in connection with this Agreement.

7.2. Without limiting the general obligations under Clause 7.1 if a Party (**Data Processor**) Processes Personal Data as a Data Processor or Sub Processor for the other Party (**Data Controller**), the Data Processor shall:

7.2.1. Process the Personal Data in accordance with Applicable Law and any other written instructions from the Data Controller (which may be specific instructions or instructions of a general nature) as set out in this Agreement or as otherwise notified in writing by the Data Controller;

7.2.2. Process the Personal Data only to the extent and in such manner as is necessary for the provision of Data Processor's obligations under this Agreement or as is required by applicable Data Protection Laws or any applicable regulatory body;

7.2.3. implement appropriate technical and organisational measures to protect the Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to the Personal Data and having regard to the nature of the Personal Data which is to be protected;

7.2.4. take reasonable steps to ensure the reliability of its staff and agents who may have access to the Personal Data;

7.2.5. obtain prior written consent from the Data Controller in order to transfer the Personal Data to any Sub-Processor (other than to Sub-Processors specified in this Agreement for whom consent is hereby granted);

7.2.6. not cause or permit the Personal Data to be transferred outside of the United Kingdom or the European Economic Area without the prior consent of the Data Controller;

7.2.7. ensure that all staff and agents required to access the Personal Data are informed of the confidential nature of the Personal Data and comply with the obligations set out in this Clause 7 (*Personal Data Protection*);

7.2.8. implement best practice and processes to minimise any risk of staff and agents publishing, disclosing or divulging any of the Personal Data to any third parties unless directed in writing to do so by the Data Controller;

7.2.9. not disclose Personnel Data to any third parties in any circumstances other than with the written consent of the Data Controller or in compliance with a legal obligation imposed upon the Data Controller; and

7.2.10. notify the Data Controller (within five (5) Working Days) if it receives a complaint or request relating to the Data Controller's obligations under applicable Data Protection Laws.

8. Intellectual Property Rights

8.1. All IPR in any materials created or developed by Cyberis solely and exclusively as a result of the provision of the Services (**Project Deliverables**) shall vest in the Client.

8.2. If, and to the extent that, any IPR in the Project Materials vest in Cyberis by operation of law, Cyberis hereby assigns all its rights (with full title guarantee and free from all third party rights) to the Client by way of a present and future assignment that shall take place immediately on the coming into existence of any such IPR

8.3. All IPR in any materials, documents, records, data, or other information provided by the Client to Cyberis for the purposes of this Agreement (**Client Background Data and Materials**) shall remain the sole and exclusive property of the Client but the Client hereby grants Cyberis royalty-free, non-exclusive and non-transferable licence to use such Client Background Data and Materials as required until termination or expiry of this Agreement for the sole purpose of enabling Cyberis to perform its obligations under this Agreement.

8.4. Subject to Clause 8.1, all other IPR in any materials, documents, records, data, or other information provided by Cyberis to the Client for the purposes of this Agreement (collectively **Cyberis Background Data and Materials**) shall remain the sole and exclusive property of Cyberis but Cyberis hereby grants the Client a royalty-free, non-exclusive and non-transferable licence to use such Cyberis Background Data and Materials as required until termination or expiry of this Agreement for the sole purpose of enabling the Client to benefit from the Services under this Agreement.

8.5. Cyberis shall indemnify, and keep indemnified, the Client in full against all costs, expenses, damages and losses (whether direct or indirect), including any interest, penalties, and reasonable legal and other professional fees awarded against or incurred or paid by the Client as a result of or in connection with any claim made against the Client for actual or alleged infringement of a third party's intellectual property arising out of, or in connection with, the supply or use of the Services, to the extent that the claim is attributable to the acts or omission of Cyberis.

8.6. The Client shall indemnify, and keep indemnified, Cyberis in full against all costs, expenses, damages and losses (whether direct or indirect), including any interest, penalties, and reasonable legal and other professional fees awarded against or incurred or paid by Cyberis as a result of or in connection with any claim made against Cyberis for actual or alleged infringement of a third party's intellectual property arising out of, or in connection with, the use of the Client Data and Materials to the extent that the claim is attributable to the acts or omission of the Client.

9. Charges, Credit Checks and Payment

9.1. The Client shall pay the Charges to Cyberis in accordance with this Clause 9 (*Charges, Credit Checks and Payment*).

9.2. Cyberis shall be entitled to charge the Client for all reasonable expenses, including but not limited to travel and subsistence, incurred by Cyberis in connection with the provision of the Services, unless expenses are explicitly excluded from the applicable Statement of Work.

9.3. The Charges are exclusive of Value Added Tax (and any other similar or equivalent taxes), which shall be payable by the Client in addition to the Charges in the manner and at the rate prescribed by law from time to time.

9.4. Subject to Clause 9.5:

9.4.1 each invoice (including for any stage payments specified in the Statement of Work) shall be payable by the Client within thirty (30) days following the date on which the invoice is received by the Client; and

9.4.2 all Charges are non-refundable.

9.5. The Client may withhold payment of any disputed Charges until the dispute is settled subject to:

9.5.1. giving Cyberis written notice of such disputed Charges within seven (7) days of receipt of the applicable invoice; and

9.5.2. paying all undisputed Charges within thirty (30) days following the date on which the invoice is received by the Client.

9.6. Notwithstanding limitations of liability specified at Clause 10 (*Liability and Insurance)*, if any undisputed Charges are not paid when properly due, Cyberis shall be entitled to charge:

9.6.1. interest daily on that sum at 3% per year above the base lending rate from time to time of Bank of England from the due date until the date of payment (whether before or after judgment); and

9.6.2. all costs (including legal costs) that Cyberis reasonably incurs to recover such overdue amounts from the Client.

9.7. Cyberis reserves the right to suspend the Services and/or any part thereof until all outstanding sums owed by the Client to Cyberis are settled.

10. Liability and Insurance

10.1. Nothing in this Agreement shall operate to exclude or restrict either Party's Liability:

10.1.1. for death or personal injury resulting from its negligence;

10.1.2. for its fraud or fraudulent misrepresentation;

10.1.3. for breach of Clause 8 (*Intellectual Property Rights*);

10.1.4. for breach of obligations arising under section 12 Sale of Goods Act 1979 or section breach of the term implied by section 2 of the Supply of Goods and Services Act 1982 (title and quiet possession); or

10.1.5. for which it is not permitted by law to exclude or limit its Liability.

10.2. Subject to Clause 10.1, neither Party (**Liable Party**) shall have any Liability to the other Party (**Claiming Party**) for any:

10.2.1. loss of profit, goodwill or revenue;

10.2.2. impact to business or loss of service as a result of any process or failure with regards to data backup and recovery services; or

10.2.3. indirect, consequential or special loss.

10.3. Subject to Clauses 10.1 and 10.2, each Party's aggregate liability in respect of any and all events under law or equity shall be limited to an amount not to exceed 125% (one hundred and twenty five percent) of the Charges under the applicable Statement of Work.

10.4. The exclusions from and limitations of Liability contained in this Agreement shall apply after as well as before the date of expiry or termination of this Agreement.

10.5. Each Party shall have satisfactory insurance cover with a reputable insurer to cover such Party's obligations and potential Liability under this Agreement and shall provide evidence of such insurance coverage at to the other Party if required to do so.

11. Confidentiality

11.1. Except as set out in Clause 11.2, each Party (**Receiving Party**) shall:

11.1.1. use the Confidential Information of the other Party (**Disclosing Party**) solely to perform the Receiving Party's obligations and to exercise the Receiving Party's rights under this Agreement;

11.1.2. keep the Disclosing Party's Confidential Information secret, safe and secure; and

11.1.3. not disclose the Disclosing Party's Confidential Information to any other person.

11.2. The Receiving Party may disclose the Disclosing Party's Confidential Information:

11.2.1. to the extent required by law, any court of competent jurisdiction or the rules of any government, public or regulatory body or any stock exchange (subject to giving the Disclosing Party written notice as soon as possible of such requirement and as permitted by law and regulation); and

11.2.2. to its officers, directors, employees, professional advisers, Affiliates, agents and sub-contractors, who need the Confidential Information in order for that Party to perform its obligations and exercise its rights under this Agreement.

11.3. The Receiving Party shall ensure that each person to whom it discloses Confidential Information under Clause 11.2 is bound by obligations of confidentiality no less onerous than those set out in this Clause 11 (*Confidentiality*).

11.4. Each Party acknowledges and agrees that damages alone may not be an adequate remedy for breach of this Clause 11 (*Confidentiality*). Accordingly, the Disclosing Party shall be entitled, without having to prove special damages, to injunctive relief, equitable relief and/or specific performance for any breach or threatened breach of this Clause 11 (*Confidentiality*).

12. Ethical Conduct

12.1. Cyberis shall conduct its business ethically and lawfully in accordance with the highest standards adhered to by similar entities operating in UK, including in accordance with the UK Cyber Security Council's Code of Ethics.

12.2. Cyberis represents and warrants that Cyberis and its subcontractors and suppliers do not use or permit unacceptable labour practices, such as child or forced labour, or unsafe working conditions and comply with all applicable labour and employment laws, regulations, standards and conventions, including the Modern Slavery Act (2015), the UN's Guiding Principles on Business & Human Rights and the International Labor Organization's Conventions.

12.3. Each Party hereby acknowledges that it is aware of, and shall comply with, all applicable anti-bribery and anti-corruption laws, including but not limited to the UK Bribery Act and the Foreign Corrupt Practices Act (FCPA) (and related regulation and guidance).

13. Compliance

13.1. Each Party shall promptly notify the other Party of any health and safety hazards which may arise in connection with this Agreement.

13.2. Cyberis shall comply with all applicable Equality Laws and shall use reasonable endeavours to comply with any reasonable equality and diversity policy provided by the Client in writing.

14. Mutual Non-Solicitation

14.1. Neither Party shall, for the duration of the Agreement and for a period of twelve (12) months thereafter, on its own account or in partnership or association with any person, firm, company or organisation or otherwise and whether directly or indirectly, solicit or entice away or attempt to solicit or entice away (or authorise the taking of any such action by any other person) any executive or worker of the other Party who has worked on the provision or use of the Services (other than subject to a normal recruitment campaign including a public advertisement of the applicable job).

15. Postponement or Cancellation

15.1. If the Client postpones or cancels a Statement of Work on ten (10) or fewer Working Days' notice prior to the Services Commencement Date then the Client shall pay the Charges to Cyberis for those cancelled Services as follows:

15.1.1. **between five (5) and ten (10) Working Days:** applicable Charges less 25%;

15.1.2. **three (3) or four (4) Working Days:** applicable Charges, less 15%; or

15.1.3. **fewer than three (3) Working Days:** applicable Charges in full.

16. Termination

16.1. Either Party may (without limiting any other remedy) at any time terminate this Agreement with immediate effect by giving written notice to the other Party if:

16.1.1. the other Party commits any material breach of this Agreement and (if capable of remedy) fails to remedy the breach within thirty (30) days after being required by written notice to do so; or

16.1.2. an order is made or a resolution is passed for the winding up of the other Party, or (in the case of an individual or firm) becomes bankrupt, makes a voluntary arrangement or composition with his or its creditors or has a receiver or administrator appointed or the other Party takes or suffers any similar or analogous action in any jurisdiction in consequence of debt.

16.2. In addition to the rights under Clause 16.2 above, Cyberis may terminate this Agreement or suspend the Services with immediate effect by giving written notice to the Client if the Client fails to make payment of any amount payable under this Agreement within sixty (60) days of the due date.

17. Notices

17.1. Formal or legal notices provided for the purposes of this Agreement shall be in writing, in English and be deemed duly given if signed by, or on behalf of, a duly authorised officer of the Party giving the notice.

17.2. Each formal or legal notice shall be delivered by courier, registered or certified mail or by hand to the relevant Party's address (or such other address which is notified to the other Party in writing from time to time).

17.3. Notices shall be deemed to have been duly given when delivered, if delivered by courier or other messenger (including registered mail) during normal Working Hours (or otherwise on commencement of the next Working Day after delivery).

17.4. Informal routine notices and communications can be by any pragmatic means agreed by the Parties.

18. General

18.1. Entire Agreement: This Agreement constitutes the entire agreement between the Parties and supersedes any prior agreement or arrangement in respect of the purposes of, and Services provided under, this Agreement.

18.2. No implied warranties or terms: Neither Party has entered into this Agreement in reliance upon, and shall have no remedy in respect of, any misrepresentation, representation or statement (whether made by the other Party or any other person) which is not expressly set out in this Agreement.

18.3. Misrepresentation: Unless such misrepresentation or warranty was made fraudulently (for which neither Party limits or excludes liability) each Party irrevocably and unconditionally waives any right it may have to claim damages for any misrepresentation whether or not contained in this Agreement and for breach of any warranty that is not specified in this Agreement.

18.4. No waiver: No waiver by either Party of any breach of this Agreement by the other Party shall be considered as a waiver of any subsequent breach of the same or any other provision. A Party's delay in exercising, partial exercising or failure to exercise a right or remedy under this Agreement shall not constitute a waiver of, or prevent or restrict future exercise of, that or any other right or remedy. A waiver of any right, remedy, breach or default shall only be valid if it is in writing and signed by the Party giving it.

18.5. No exclusion of fraud: Nothing in Clause 10 (*Liability and Insurance*) (or elsewhere is this Agreement) shall limit, exclude (nor be deemed to limit or exclude) the liability of either Party for fraud or fraudulent misrepresentation.

18.6. Unenforceable provisions: If any provision of this Agreement is found by any court or body or authority of competent jurisdiction to be illegal, unlawful, void or unenforceable, such provision shall be deemed to be severed from this Agreement and this shall not affect the remainder of this Agreement which shall continue in full force and effect.

18.7. Variations: Except to the extent otherwise specified in this Agreement, variations to this Agreement shall be agreed in writing and duly executed by both Parties.

18.8. No partnership: No partnership, agency or joint venture between the Parties shall be created by this Agreement.

18.9. Independent Contractors: Each Party is an independent contractor and is entering into this Agreement as principal and not as agent for or for the benefit of any other person.

18.10. Third Party Rights: The Parties do not intend that any provision of this Agreement shall be enforceable under the Contracts (Rights of Third Parties) Act 1999 by any person other than a Party to this Agreement.

18.11. No assignment: Neither Party shall assign, transfer, charge, hold on trust for any person or deal in any other manner with any of such Party's rights under this Agreement other than either Party may, on ten (10) Working Days' written notice to the other Party, assign the whole of this Agreement to a wholly owned Affiliate of such Party.

18.12. Force Majeure: Neither Party shall be liable to the other Party for failure to perform its obligations under this Agreement if such failure results from an event of Force Majeure. Each Party shall promptly notify the other Party of the occurrence of any event of Force Majeure. If the event of Force Majeure continues for a period of two months or longer, either Party may then terminate this Agreement without fault.

19. Governing Law, Jurisdiction and ADR

19.1. This Agreement and any non-contractual obligations or rights arising in connection with it are governed by the laws of England. The courts of England have exclusive jurisdiction to determine any dispute arising in connection with this Agreement.

19.2. In the event of a Dispute arising in relation to the provision of the services in this Agreement, the Parties shall initially attempt to resolve by good faith negotiations for at least fifteen (15) Working Days but thereafter shall (if both Parties agree to do so within fifteen (15) Working Days or being requested to do so by the other Party) be subject to Alternate Dispute Resolution through a registered ADR authority based in the United Kingdom.

19.3. Each Party shall be liable for their own costs arising from ADR exclusively and in no way shall be liable for costs arising through the use of ADR for the other Party.

19.4. If the Parties do not agree to ADR in accordance with Clause 19.2 either Party may then take the Dispute to the applicable Courts.

CYBER SECURITY INCIDENT RESPONSE RETAINER SERVICES TERMS (CSIR RETAINER SERVICES TERMS)

1. Applicability

These CSIR Retainer Services Terms only apply if the Client purchases CSIR Retainer Services.

2. Definitions and Interpretation

2.1. The following words and phrases have the following meanings in these CSIR Retainer Services Terms:

WORD OR PHRASE	DEFINITION
Authorised Client Personnel:	means those individually named employees, agents and independent contractors of the Client who have the necessary skills and authority to make decisions and who are nominated by the Client as being authorised to use the CSIR Retainer Services.
CSIR Retainer Services:	Has the meaning given in Section 5 (*CSIR Retainer Services*) below.
CSIR Retainer Services Hours:	means the purchased hours as detailed in the Statement of Works which cover the following activities (in fifteen (15)-minute increments with a minimum of 1 hour per assistance request) during the CSIR Retainer Services Term of twelve (12) months: • verbal triage calls; • time spent conducting remote or onsite analysis and support; • incident analysis and management activities; • travel time for attending onsite response requests; • time spent compiling an incident report; and • post-incident review meetings.
	Working hours of individual Cyberis incident response consultants will not exceed twelve (12) consecutive working hours in a twenty-four (24)-hour period.
CSIR Retainer Services Term:	Has the meaning given in Section 3 (*CSIR Retainer Term*) below.
Forensics Data:	means host and network-based data such as memory, disk, logs, data, and historic or real time network traffic as well as any malware.
Incident Response Request:	means the event when a request for incident response assistance is reported by the Client to Cyberis via telephone, web or email.

3. CSIR Retainer Services Term

3.1. Cyberis shall provide the CSIR Retainer Services for twelve (12) months (**CSIR Retainer Services Term**) from the date of each applicable Purchase Order or Contract Acceptance Form. If an incident investigation has begun but is not completed on or before the expiry of the CSIR Retainer Services Term, the CSIR Retainer Services Term will be extended automatically so that it will expire sixty (60) days after the incident investigation is complete.

4. CSIR Retainer Services Locations

4.1. Services will be performed by Cyberis personnel for the Client locations detailed in the Statement of Works. Services may also be provided from, or for, a location not detailed in the Statement of Works subject to Cyberis' prior written approval on a case-by-case basis.

5. CSIR Retainer Services

5.1. Cyberis will use different strategies and methodologies to complete the CSIR Retainer Services depending on the nature of the cyber security incident as outlined in this Section 5 (collectively the **CSIR Retainer Services**). Cyberis will consult with Authorised Client Personnel at the outset of the investigation to identify initial objectives and regularly thereafter throughout the engagement to discuss updates

to those objectives and other investigation decisions. Client will make any material decisions on investigation strategy.

5.2. CSIR Retainer Services may include Cyberis conducting the activities below, but the Client acknowledges and agrees that in providing the CSIR Retainer Services, Cyberis may modify its approach as appropriate to assist the Client in investigating a potential cyber security incident:

5.2.1. incident triage and identification;

5.2.2. advice towards defining the objectives of the incident response operation;

5.2.3. advice to and management of internal incident responders, where required;

5.2.4. advice regarding informing and co-operating with regulators, interested parties and law enforcement, where appropriate and possible;

5.2.5. advice and management of incident response services offered by cyber security insurance providers;

5.2.6. advice towards crisis communications;

5.2.7. host-based intrusion analysis, where access to systems is available;

5.2.8. network-based intrusion analysis where network information sources are available;

5.2.9. basic live analysis of malware samples;

5.2.10. advice regarding containment and eradication of infections, where appropriate and possible;

5.2.11. design of IoC signatures for detective and protective devices within the affected organisation, where practical;

5.2.12. post-incident reporting to the incident investigated; and

5.2.13. post-incident briefing for executives and stakeholders.

5.3. Cyberis makes no representation or warranty that performance of analysis activities will detect all malware, malicious software or anomalies which may be present on Client systems and networks (collectively **Threats**). Cyberis accepts no liability for failing to identify Threats where such Threats exist or are subsequently identified in systems previously assessed.

6. Documented Reports

6.1. In connection with an incident investigation, if and as requested by the Client, Cyberis will deliver one or more of the following documents:

6.1.1. a detailed timesheet of the work conducted, provided as standard at the end of the support provided;

6.1.2. Incident Response Report documenting pertinent data revealed during the investigation, affected systems, network, or data assets compromised, a full analysis of adversary activities where this can be extrapolated and a root-cause analysis (if known); and/or

6.1.3. Management Briefings summarising pertinent information for use in briefing senior executive staff.

6.2. Cyberis will discuss with Client the proposed content of any documented reports in advance of production or sharing. Such reports typically require up to five Working Days for production and review. The reports will be provided to the Client Authorised Personnel, as applicable, and Cyberis will not be required to provide reports or documentation (or copies of them) to any other party or individual.

7. Post-Incident Reviews

7.1. In connection with an incident investigation, if and as requested by the Client, Cyberis will participate in a post-incident review which aims to:

7.1.1. ensure lessons are learned about how the incident unfolded;

7.1.2. highlight how the incident response process could be improved internally; and

7.1.3. what changes to technology, people or processes could be incorporated to prevent recurrence of the incident or lessen the impact of any future incident.

7.2. During this debrief, all evidence and activities will be discussed with the teams involved in the incident response effort.

8. Outstanding CSIR Retainer Services Hours

8.1. At the end of the twelve (12)-month CSIR Retainer Services Term, if outstanding CSIR Retainer Services Hours remain, there is a three (3)-month grace period in which those outstanding CSIR Retainer Services Hours may be used for the delivery of Cyberis' other services, for example:

8.1.1. tabletop exercises;

8.1.2. development of related technical process documentation;

8.1.3. creation of incident response playbooks detailing specific response actions;

8.1.4. cyber security incident response plan enhancements;

8.1.5. incident response training; and/or

8.1.6. other regular scheduled technical assurance services, for example, web application penetration testing.

8.2. Delivery of any such consulting services are subject to mutual agreement between the Parties with respect to the scope of the consulting services, any additional terms, and timing of delivery. Cyberis will provide the Client with a corresponding proposal describing the agreed consulting services, and the Client must sign and return a Contract Acceptance Form prior to commencing of any such consulting services. The Service Level Agreements shall not apply to any such consulting services.

9. Out of scope

9.1. Cyberis will perform the CSIR Retainer Services with reasonable care and skill; however, nothing in this Agreement serves as a guarantee the CSIR Retainer Services will detect or identify all security or network threats, vulnerabilities or intrusions, decrypt or recover data, restore operations or return control of Client Property where unauthorised access or control has occurred. Applicable law or regulation(s) of the country in which CSIR Retainer Services will be performed may limit or alter the scope of the CSIR Retainer Services that can be provided in that country, in which case the Parties will work collaboratively to determine the best course of action.

9.2. The following (without limitation) are not in-scope for the CSIR Retainer Services:

9.2.1. expert testimony or litigation assistance or support services;

9.2.2. hands-on configuration of systems and security controls;

9.2.3. rebuilding / reimaging of affected systems;

9.2.4. implementation of a remediation plan, detective and preventative controls, and reconfiguring of such controls; or

9.2.5. provision of any regulated service or activities.

9.3. Cyberis is not licensed or certified in any country, state, or province as a private investigator, legal advisor, auditor, or licensed or certified engineer and is not being retained to provide private investigatory services, legal advice, audit or internal control advisory services, or engineering services that would require a license or certification.

9.4. The following activities fall outside of the scope for the Services, but can be delivered at an additional cost:

9.4.1. internal and external communications;

9.4.2. detailed digital forensics of affected systems (note, that forensically-sound acquisition of devices may incur additional delays in arrangement);

9.4.3. detailed malware reverse engineering; and

9.4.4. deployment of network monitoring capabilities.

10. Deployment of Equipment and Software

10.1. Cyberis may be required to deploy and connect equipment, software, tools and scripts to the Client systems and networks and, in doing so, Cyberis shall use reasonable endeavours not to interfere with, or interrupt, any Client Property. Any hardware or software provided by Cyberis for installation on Client Property remains the property of Cyberis or its licensors.

10.2. Any third-party tools used by Cyberis to provide the CSIR Retainer Services may subject to additional terms which Cyberis shall provide to the Client via email to the Client Authorised Personnel.

10.3. The Client may be required to install software on any agreed systems and networks, in accordance with Cyberis' instructions. Cyberis shall not have any liability in the event that damage, loss, corruption, or interruption is caused to Client networks, systems, data, and services by such deployments.

10.4. The Client shall cooperate with Cyberis to remove, or upon request of Cyberis, promptly return any of Cyberis' physical devices and software installed on the Client's premises, systems or networks and confirm removal of any Cyberis software from Client devices.

11. Client Responsibilities

11.1. The Client shall be solely responsible for providing or obtaining consent for Cyberis to collect and analyse host and network-based data such as memory, disk, logs, data, and historic or real time network traffic as well as any malware (collectively **Forensics Data**), and archiving, analysing, and retaining all Forensics Data captured or obtained as part of CSIR Retainer Services.

11.2. If the Client fails to obtain any such consents, the Client shall be solely and fully responsible for any related claims or liabilities.

11.3. The Client authorises Cyberis to collect and perform any off-site analysis of Forensics Data as necessary for the delivery of the CSIR Retainer Services.

11.4. The Client will ensure the timely provision of out-of-band communications systems and forensic imaging.

11.5. There is inherent risk in incident response activities, which may lead to operational degradation, performance impact, incidents of non-compliance with internal policies or industry standards, data loss or other impairment of Client Property, or downstream effects. The Client will work with Cyberis to help reduce the risk of damage to Client Property or impact to Client operations resulting from incident investigation activities. As long as Cyberis is using reasonable care in the performance of the CSIR Retainer Services, Cyberis will not be liable for any such damage or impacts arising out of the CSIR Retainer Services.

12. Service Level Agreement

12.1. The following Service Levels (**SLA**) shall apply to CSIR Retainer Services:

CSIR RETAINER SERVICES FEATURE	CSIR RETAINER SERVICES FEATURE DESCRIPTION
24/7 phone access:	the Client will have access to a 24/7 phone number to contact Cyberis' Incident Response Team to request incident response assistance (**Incident Response Request**).
Additional Service Hours:	additional service hours can be pre-purchased prior to a security incident occurring in increments of 10 CSIR Service Hours.
CSIR Retainer Service Management:	Cyberis will assign an Account Manager to the Client who will manage the CSIR Retainer Services outside of open incident responses, capture general feedback formally and conduct CSIR Retainer Services reviews with the Client. This is designed to provide ongoing quality assurance across each twelve (12)-month CSIR Retainer Services Term.
Onsite Support:	where applicable, Cyberis will commence onsite support at pre-agreed locations within twenty-four (24) hours of ending the initial Verbal Triage. If Cyberis does not launch onsite support within those twenty-four (24) hours, Cyberis shall credit the Client with 1 CSIR Retainer Service Credit. If the location is not pre-agreed, Cyberis will commence onsite support as soon as practically possible.
Post-Incident Review:	if requested and subject to availability, Cyberis will participate in a post-incident review within five (5) Working Days of report delivery. If Cyberis does not attend such scheduled post-incident review, Cyberis shall credit the Client with one (1) CSIR Service Credit.
Remote Support:	where applicable, Cyberis will commence remote support for the Incident Response Request within eight (8) hours after the initial Verbal Triage. If Cyberis does not launch remote support within those eight (8) hours, Cyberis shall credit the Client with 1 CSIR Service Credit.
Reporting:	if requested upon the completion of an incident investigation, Cyberis shall produce an incident report that will be delivered within five (5) Working Days. If Cyberis does not deliver an incident report within those five (5) Working Days, Cyberis shall credit the Client with one (1) CSIR Service Credit.
Verbal Triage:	Cyberis' Incident Response Team will respond to the Client's Incident Response Request within four (4) hours (**Verbal Triage**). If Cyberis do not respond to the Client Incident

CSIR RETAINER SERVICES FEATURE	CSIR RETAINER SERVICES FEATURE DESCRIPTION
	Response Request within those four (4) hours, Cyberis shall credit the Client with one (1) CSIR Retainer Service Credit.
Zero-config VPN Device:	Cyberis shall supply the Client a zero-config VPN device at the commencement of the twelve (12)-month CSIR Retainer Services Term to provide Cyberis remote network connectivity.

12.2. A CSIR Retainer Service Credit shall equal 2.5% of the annual Charge for the CSIR Retainer Services or a minimum of £500 (whichever is greater). Credit will be issued towards the next invoice due for the CSIR Retainer Services after submission of a CSIR Service Credit request, or if no additional invoice is due, as a payment. The Client must submit a CSIR Retainer Service Credit request to the nominated Account Manager within 10 Working Days of the end of the calendar month in which the suspected Service Level Agreement non-compliance occurred.

12.3. If a systemic cyber event that impacts more than five organisations or businesses within a forty-eight (48)-hour period (for example a widespread malware outbreak or a distributed denial of service attack that impacts multiple organisations or geographic regions), Cyberis will not be able to provide dedicated on-site IR support to all retained clients. In such event, Cyberis will make reasonable efforts to provide remote centrally coordinated support across multiple clients, where logistically possible either via technical remote access or simply via telephone communication, and the on-site support SLA shall not apply.

12.4. Cyberis will not be responsible for any delay or inability to perform Services due to an event of Force Majeure.

13. Expenses

13.1. Any Cyberis consultant travel and subsistence expenses will be recharged at cost.

14. Cancellation

14.1. If the Client wishes to cancel the CSIR Retainer Services during an unexpired CSIR Retainer Services Term, Charges that have already been paid or are owing will not be refunded or credited.

15. Conflict of Interest

15.1. The Client acknowledges that Cyberis may be providing separate services to the Client that may in some way relate to an incident investigation. Provided that Cyberis implements reasonable procedures to mitigate any potential conflict of interest, the Client will not make claims against Cyberis alleging conflict of interest.

16. Termination of an Incident Investigation

16.1. Notwithstanding anything in the Agreement to the contrary, either Party can terminate any incident investigation (but not this Agreement in entirety) by providing five (5) Working Days' written notice to the other Party.

CONTINUOUS VULNERABILITY ASSESSMENT SERVICES (CVA SERVICES TERMS)

1. Applicability

These CVA Services Terms only apply if the Client purchases CVA Services.

2. Definitions and Interpretation

2.1. The following words and phrases have the following meanings in these CVA Services Terms:

WORD OR PHRASE	DEFINITION
Assessed Asset:	means any Asset that has been scanned by Cyberis for a vulnerability, configuration, or state.
Asset:	means: • a physical or virtual device with an operating system connected to a network; • a web application with an FQDN; or • an active (not terminated) Cloud resource (including but not limited to containers, virtual devices, applications, native services, etc.) that can be actively or passively assessed. Assets may include, but are not limited to: laptops, desktops, servers, routers, firewalls, switches, IoT devices, mobile phones, virtual machines, software containers, operational technology devices and cloud resources.
CVA Services:	means the Continuous Vulnerability Assessment Services managed by Cyberis and provided Tenable, Inc. software and services.
CVA Services Interruption Time:	means the period of time for which the CVA Services (or any material portion thereof) are unavailable due to issues caused by or attributable to Cyberis or its agents. CVA Services Interruption Time does not include Regular Maintenance or Scheduled Maintenance.
Discovered Asset:	means any Asset that has been identified by discovery plugins, but not scanned for vulnerability, configuration or state.
Emergency Maintenance:	means maintenance for certain emergency situations, where advance notice may not be feasible, possible or practical. Cyberis shall use commercially reasonable efforts to minimise any Emergency Maintenance windows to the minimum time necessary to support performance of the CVA Services. Periods of Emergency Maintenance shall be included in Services Interruption Time.
Exclusion:	means any time for which the CVA Services are unavailable to do any of the following: • the Client's breach of, or failure to perform any obligations under, this Agreement; • issues relating to the Client's environment, internal networks, computer systems, firewalls or the Client's inability to connect to the internet; • Force Majeure; or • issues arising from failures, acts or omissions of Tenable's upstream service providers (i.e. AWS).
Licensed Asset:	means any Asset that has been assessed by Cyberis as part of the CVA Services within the preceding ninety (90)-days.
Potential Uptime:	means the amount of time in a given month.
Production Uptime:	means the amount of time in a given month that the Client has the ability to log in or access the CVA Services user interface (or authenticate to APIs) and perform associated scanning related activity. Production Uptime is measured by Cyberis in a given month by the following calculation: *Production Uptime = (Potential Uptime) – (CVA Services Interruption Time) / (Potential Uptime) – (Exclusions).*

WORD OR PHRASE	DEFINITION
Regular Maintenance:	means the period of time during which the CVA Services may be unavailable to allow for recurring maintenance work. Tenable attempts to schedule this time when usage of the CVA Services is light across Tenable's customer base and therefore, Tenable shall use commercially reasonable efforts to only conduct Regular Maintenance daily between the hours of 7AM and 9AM (ET) and non-business days. Regular Maintenance is required in order to update Tenable's plug-in databases as well as to maintain system health requirements. Tenable shall use commercially reasonable efforts to minimise any Regular Maintenance windows to the minimum time necessary to support performance of the CVA Services. Often times, the Client will not experience any CVA Services Interruption Time during periods of Regular Maintenance.
Scheduled Maintenance:	means the period of time during which the CVA Services may be unavailable for non-recurring maintenance. Scheduled Maintenance is required in order to provide updates to the CVA Services as well as to maintain system health requirements. Cyberis shall provide the Client at least twelve (12) hours advance notice prior to Scheduled Maintenance; provided, however, Tenable shall endeavour to provide at least twenty-four (24) hours advanced notice for Scheduled Maintenance. Notice for Scheduled Maintenance will be provided at the following URL or successor location: status.tenable.com. Tenable shall use commercially reasonable efforts to minimise any Scheduled Maintenance windows to the minimum time necessary to support performance of the CVA Services. Often times, the Client will not experience any CVA Services Interruption Time during periods of Scheduled Maintenance.
Tenable	means Tenable, Inc – a company that supplies software and services that comprise elements of the CVA Services.

3. Software Licence Agreements for CVA Services

3.1. Cyberis will enter into the licence agreements with Tenable, Inc. in order to implement the CVA Services and the Client shall accept and comply with such terms as specified at: https://static.tenable.com/prod_docs/tenable_slas.html.

3.2. Cyberis shall provide the Client with technical guidance designed to ensure the Tenable components are configured in line with best practices. Where components are configured within the Client's environment, it will be the responsibility of the Client to implement that technical guidance.

4. System Availability and Business Interruption

4.1. Cyberis shall not be responsible if the use of any Tenable products that Cyberis provides as part of the CVA Services impacts availability of any Client systems and/or causes business interruption.

4.2. The Client shall inform Cyberis within five (5) Working Days of any time periods where vulnerability scans, Tenable configuration changes or Tenable software updates cannot be applied.

5. Service Level Agreement

5.1. The Client understands that assessing network security is a complex procedure, and Cyberis does not guarantee that the results of the CVA Services will be error-free or provide a complete and accurate picture of the Client's security flaws.

5.2. Cyberis shall provide a 99.95% Production Uptime with respect to the CVA Services during each calendar month during the Term (Service Level Agreement).

5.3. If the CVA Services do not meet the Service Level Agreement (unless due to an Exclusion), then the Client may request a Service Level Credit. The Weighting Factor for calculation of the Service Level Credit correlates to the relative unavailability of the CVA Services in a given month as follows:

- Production Uptime between 99.95% and 100% = 0;
- Production Uptime between 95.00% and 99.94% = .1;
- Production Uptime between 90.00% and 94.99% = .15;
- Production Uptime below 90% = .2.

5.4. The following equation shall be used to calculate any Service Level Credits:

Service Level Credit (in £) = Weighting Factor multiplied by the monthly Charges.

Example: Production Uptime in a given month is 95%. The Monthly Fee for the CVA Services is £100 (Annual fee for the CVA Services is £1,200). Service Level Credit (in £) = (0.1) x £100 = £10. Monthly fees will be calculated on a pro rata basis.

5.5. In order to receive a Service Level Credit, the Client must email Cyberis within five (5) calendar days of the end of the applicable month.

5.6. If the CVA Services Charges are past due or the Client is in default with respect to any payment or any material contractual obligations to Cyberis, the Client is not eligible for any Service Level Credit.

5.7. Service Level Credits may only be applied to future upgrades or renewals of the specific CVA Services affected (and will not result in any refund of Charges).

6. Light Collection Mode and Personal Data Protection for CVA Services

6.1. Light Collection Mode minimises Personal Data collected by Plug-ins during Scans. In Light Collection Mode, Tenable plugins anonymise Personal Data so that it is not collected or stored in Tenable systems. The Client must inform Cyberis in writing if Light Collection Mode is required.

7. Licence Shortfall

7.1. Additional Licenced Assets can be purchased where required. The Client shall immediately purchase any shortfall of the Licensed Assets that is identified by Cyberis.

8. Troubleshooting

8.1. In order to better assist in troubleshooting issues raised, Cyberis may have to engage Tenable for support, and Tenable may have to log into the associated Client account as part of this. If this is required, Tenable will only access the account:

8.1.1. to provide support in connection with the raised issue; and

8.1.2. for the amount of time required to resolve the raised issue.

8.2. Tenable will not make any changes to the Client account without written permission from Cyberis.

9. Consequences of Expiry or Early Termination

9.1. On expiry or earlier termination of CVA Services Term, the Client shall remove all Tenable related components from the Client environments.

10. No Cancellation

10.1. Clause 15 (*Postponement or Cancellation*) of Cyberis Standard Terms will not apply to CVA Services and so, if the Client wishes to cancel the CVA Services during an unexpired CVA Services Term, Charges that have already been paid or are owing will not be refunded or credited.