www.cqc.org.uk

Contract (Short Form – Services)

Contract for Healthwatch England Sites Penetration Testing

Contract Reference CQC ICTC 672

August 2017

Contents

THIS CONTRACT is dated 26th of September 2017

PARTIES

(1) CARE QUALITY COMMISSION of 151 Buckingham Palace Road, London, SW1W 9SZ 2HQ (**"the Customer"**).

And

(2) 7 Safe Limited whose registered office is at 123 Buckingham Palace Road, London, SW1W 9SR (Company Number 04274874)(**"the Contractor"**)

(Together the **"Parties"**)

Background

1. The Customer is the independent health and social care regulator in England that monitors, inspects and regulates health and social care services to ensure they meet fundamental standards of quality and safety. It ensures health and social care services provide people with safe, effective, compassionate, high-quality care and we encourage care services to improve.
2. The Customer requires a scope of work for carrying out blackbox, greybox and API assessment for their Healthwatch CRM web applications.
3. The Contractor has been appointed by the Customer to provide the Services.
4. Therefore the Parties have agreed to enter into this Contract for the provision of the services defined in the Agreement.

1 Interpretation

1.1 In these terms and conditions:

"Agreement"	means the contract consisting of these terms and conditions, any attached Schedules, the invitation to tender including Specification, the Tender Response between (i) the Care Quality Commission ("Customer") and (ii) 7 Safe ("Contractor");
"Approval"	means the written consent of the Customer;
"Central Government Body"	means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: (a) Government Department; (b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); (c) Non-Ministerial Department; or (d) Executive Agency;
"Charges"	means the charges for the Services as specified in the Schedule 2;
"Confidential Information"	means all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which (i) is known by the receiving Party to be confidential; (ii) is marked as or stated to be confidential; or (iii) ought reasonably to be considered by the receiving Party to be confidential;
"Contractor"	means the person named as Contractor who was awarded this contract;
"Customer"	means the Care Quality Commission;
"DPA"	means the Data Protection Act 1998;
"Expiry Date"	means the date for expiry of the Agreement as set out in the

	Schedule 1 ;
“FOIA”	means the Freedom of Information Act 2000;
“Information”	has the meaning given under section 84 of the FOIA;
“Key Personnel”	means any persons specified as such in the Specification or Agreement otherwise notified as such by the Customer to the Contractor in writing;
Open Source Software	means computer software, computer program, source code and any other material that is published for use, with rights to access and modify, by any person for free under a generally recognised open source licence.
“Party”	means the Contractor or the Customer (as appropriate) and “Parties” shall mean both of them;
“Personal Data”	means personal data (as defined in the DPA) which is processed by the Contractor or any Staff on behalf of the Customer pursuant to or in connection with this Agreement;
“Premises”	means the location where the Services are to be supplied, as set out in the Specification;
“Purchase Order Number”	means the Customer’s unique number relating to the supply of the Services by the Contractor to the Customer in accordance with the terms of the Agreement;
“Request for Information”	has the meaning set out in the FOIA or the Environmental Information Regulations 2004 as relevant (where the meaning set out for the term “request” shall apply);
“Schedule”	means a schedule attached to, and forming part of, the Agreement;
“Services”	means the services to be supplied by the Contractor to the Customer under the Agreement;
“Specification”	means the specification for the Services (including as to quantity, description and quality) as specified in Schedule 1;
“Staff”	means all directors, officers, employees, agents, consultants and contractors of the Contractor and/or of any sub-contractor of the Contractor engaged in the performance of the Contractor’s

	obligations under the Agreement;
"Staff Vetting Procedures"	means vetting procedures that accord with good industry practice or, where requested by the Customer, the Customer's procedures for the vetting of personnel as provided to the Contractor from time to time;
"Tender Response"	Means the Contractor's response to the Customer's invitation to tender and attached at Schedule 3;
"Term"	means the period from the start date of the Agreement set out in the Schedule 1 to the Expiry Date as such period may be extended in accordance with clause 4.2 or terminated in accordance with the terms and conditions of the Agreement;
"VAT"	means value added tax in accordance with the provisions of the Value Added Tax Act 1994; and
"Working Day"	means a day (other than a Saturday or Sunday) on which banks are open for business in the City of London.

1.2 In these terms and conditions, unless the context otherwise requires:

1.2.1 references to numbered clauses are references to the relevant clause in these terms and conditions;

1.2.2 any obligation on any Party not to do or omit to do anything shall include an obligation not to allow that thing to be done or omitted to be done;

1.2.3 the headings to the clauses of these terms and conditions are for information only and do not affect the interpretation of the Agreement;

1.2.4 any reference to an enactment includes reference to that enactment as amended or replaced from time to time and to any subordinate legislation or byelaw made under that enactment; and

1.2.5 the word 'including' shall be understood as meaning 'including without limitation'.

2 Priority of documents

2.1 In the event of, and only to the extent of, any conflict between the clauses of the Agreement, any document referred to in those clauses and the Schedules, the conflict shall be resolved in accordance with the following order of precedence:

a) these terms and conditions

b) the Schedules

c) any other document referred to in these terms and conditions

3 Supply of Services

3.1 In consideration of the Customer's agreement to pay the Charges, the Contractor shall supply the Services to the Customer for the Term subject to and in accordance with the terms and conditions of the Agreement.

3.2 In supplying the Services, the Contractor shall:

3.2.1 co-operate with the Customer in all matters relating to the Services and comply with all the Customer's instructions;

3.2.2 perform the Services with all reasonable care, skill and diligence in accordance with good industry practice in the Contractor's industry, profession or trade;

3.2.3 use Staff who are suitably skilled, experienced and possess the required qualifications to perform tasks assigned to them, and in sufficient number to ensure that the Contractor's obligations are fulfilled in accordance with the Agreement;

3.2.4 ensure that the Services shall conform with all descriptions and specifications set out in the Specification;

3.2.5 comply with all applicable laws; and

3.2.6 provide all equipment, tools and vehicles and other items as are required to provide the Services.

3.3 The Customer may by written notice to the Contractor at any time request a variation to the scope of the Services. If the Contractor agrees to any variation to the scope of the Services, the Charges shall be subject to fair and reasonable adjustment to be agreed in writing between the Customer and the Contractor.

4 Term

4.1 The Agreement shall take effect on the date specified in Schedule 1 and shall expire on the Expiry Date, unless it is otherwise extended in accordance with clause 4.2 or terminated in accordance with the terms and conditions of the Agreement.

4.2 The Customer may extend the Agreement for a period of up to 6 months by giving not less than 10 Working Days' notice in writing to the Contractor prior

to the Expiry Date. The terms and conditions of the Agreement shall apply throughout any such extended period.

5 Charges, Payment and Recovery of Sums Due

5.1 The Charges for the Services shall be as set out in the Tender Response appended hereto in Schedule 2 and shall be the full and exclusive remuneration of the Contractor in respect of the supply of the Services. Unless otherwise agreed in writing by the Customer, the Charges shall include every cost and expense of the Contractor directly or indirectly incurred in connection with the performance of the Services.

5.2 The Contractor shall invoice the Customer as specified in the Agreement. Each invoice shall include such supporting information required by the Customer to verify the accuracy of the invoice, including the relevant Purchase Order Number and a breakdown of the Services supplied in the invoice period.

5.3 In consideration of the supply of the Services by the Contractor, the Customer shall pay the Contractor the invoiced amounts no later than 30 days after receipt of a valid invoice which includes a valid Purchase Order Number. The Customer may, without prejudice to any other rights and remedies under the Agreement, withhold or reduce payments in the event of unsatisfactory performance.

5.4 All amounts stated are exclusive of VAT which shall be charged at the prevailing rate. The Customer shall, following the receipt of a valid VAT invoice, pay to the Contractor a sum equal to the VAT chargeable in respect of the Services.

5.5 If there is a dispute between the Parties as to the amount invoiced, the Customer shall pay the undisputed amount. The Contractor shall not suspend the supply of the Services unless the Contractor is entitled to terminate the Agreement for a failure to pay undisputed sums in accordance with clause 16.4. Any disputed amounts shall be resolved through the dispute resolution procedure detailed in clause 19.

5.6 If a payment of an undisputed amount is not made by the Customer by the due date, then the Customer shall pay the Contractor interest at the interest rate specified in the Late Payment of Commercial Debts (Interest) Act 1998.

5.7 If any sum of money is recoverable from or payable by the Contractor under the Agreement (including any sum which the Contractor is liable to pay to the Customer in respect of any breach of the Agreement), that sum may be deducted unilaterally by the Customer from any sum then due, or which may come due, to the Contractor under the Agreement or under any other

agreement or contract with the Customer. The Contractor shall not be entitled to assert any credit, set-off or counterclaim against the Customer in order to justify withholding payment of any such amount in whole or in part.

5.8 Where the Contractor enters into a sub-contract, the Contractor shall include in that sub-contract:

5.8.1 Provisions having the same effect as clauses 5.2 to 5.6 of the Agreement and

5.8.2 Provisions requiring the counterparty to that subcontract to include in any sub-contract which it awards provisions having the same effect as clauses 5.2 to 5.6 of this Agreement

5.8.3 In this clause 5.8 'sub-contract' means a contract between two or more suppliers, at any stage of remoteness from the Customer in a sub-contracting chain, made wholly or substantially for the purpose of performing (or contributing to the performance of) the whole or any part of this Agreement.

6 Premises and equipment

6.1 If necessary, the Customer shall provide the Contractor with reasonable access at reasonable times to its premises for the purpose of supplying the Services. All equipment, tools and vehicles brought onto the Customer's premises by the Contractor or the Staff shall be at the Contractor's risk.

6.2 If the Contractor supplies all or any of the Services at or from the Customer's premises, on completion of the Services or termination or expiry of the Agreement (whichever is the earlier) the Contractor shall vacate the Customer's premises, remove the Contractor's plant, equipment and unused materials and all rubbish arising out of the provision of the Services and leave the Customer's premises in a clean, safe and tidy condition. The Contractor shall be solely responsible for making good any damage to the Customer's premises or any objects contained on the Customer's premises which is caused by the Contractor or any Staff, other than fair wear and tear.

6.3 If the Contractor supplies all or any of the Services at or from its premises or the premises of a third party, the Customer may, during normal business hours and on reasonable notice, inspect and examine the manner in which the relevant Services are supplied at or from the relevant premises.

6.4 The Customer shall be responsible for maintaining the security of its premises in accordance with its standard security requirements. While on the Customer's premises the Contractor shall, and shall procure that all Staff shall, comply with all the Customer's security requirements.

6.5 Where all or any of the Services are supplied from the Contractor's premises, the Contractor shall, at its own cost, comply with all security requirements specified by the Customer in writing.

6.6 Without prejudice to clause 3.2.6, any equipment provided by the Customer for the purposes of the Agreement shall remain the property of the Customer and shall be used by the Contractor and the Staff only for the purpose of carrying out the Agreement. Such equipment shall be returned promptly to the Customer on expiry or termination of the Agreement.

6.7 The Contractor shall reimburse the Customer for any loss or damage to the equipment (other than deterioration resulting from normal and proper use) caused by the Contractor or any Staff. Equipment supplied by the Customer shall be deemed to be in a good condition when received by the Contractor or relevant Staff unless the Customer is notified otherwise in writing within 5 Working Days.

6.8 Any Premises/land made available from time to time to the Contractor by the Customer in connection with the contract, shall be made available to the contractor on a non-exclusive licence basis free of charge and shall be used by the contractor solely for the purpose of performing its obligations under the contract. The Contractor shall have the use of such Premises/land as licensee and shall vacate the same on completion, termination or abandonment of the Contract.

6.9 The Parties agree that there is no intention on the part of the Customer to create a tenancy of any nature whatsoever in favour of the Contractor or its Staff and that no such tenancy has of shall come into being and, notwithstanding any rights granted pursuant to the Contract, the Customer retains the right at any time to use any premises owned or occupied by it in any manner it sees fit.

6.10 Should the Contractor require modifications to the Premises, such modifications shall be subject to prior Approval and shall be carried out by the Customer at the Contractor's expense. The Customer shall undertake approved modification work without undue delay. Ownership of such modifications shall rest with the Customer.

6.11 All the Contractor's equipment shall remain at the sole risk and responsibility of the Contractor, except that the Customer shall be liable for loss of or damage to any of the Contractor's property located on Customers Premises which is due to the negligent act or omission of the Customer.

7 Staff and Key Personnel

7.1 If the Customer reasonably believes that any of the Staff are unsuitable to undertake work in respect of the Agreement, it may, by giving written notice to the Contractor:

7.1.1 refuse admission to the relevant person(s) to the Customer's premises;

7.1.2 direct the Contractor to end the involvement in the provision of the Services of the relevant person(s); and/or

7.1.3 require that the Contractor replace any person removed under this clause with another suitably qualified person and procure that any security pass issued by the Customer to the person removed is surrendered,

and the Contractor shall comply with any such notice.

7.2 The Contractor shall:

7.2.1 ensure that all Staff are vetted in accordance with the Staff Vetting Procedures; and if requested, comply with the Customer's Staff Vetting Procedures as supplied from time to time;

7.2.2 if requested, provide the Customer with a list of the names and addresses (and any other relevant information) of all persons who may require admission to the Customer's premises in connection with the Agreement; and

7.2.3 procure that all Staff comply with any rules, regulations and requirements reasonably specified by the Customer.

7.3 Any Key Personnel shall not be released from supplying the Services without the agreement of the Customer, except by reason of long-term sickness, maternity leave, paternity leave, termination of employment or other extenuating circumstances.

7.4 Any replacements to the Key Personnel shall be subject to the prior written agreement of the Customer (not to be unreasonably withheld). Such replacements shall be of at least equal status or of equivalent experience and skills to the Key Personnel being replaced and be suitable for the responsibilities of that person in relation to the Services.

7.5 At the Customer's written request, the Contractor shall provide a list of names and addresses of all persons who may require admission in connection with the Contract to the Premises, specifying the capacities in

which they are concerned with the Contract and giving such other particulars as the Customer may reasonably request.

7.6 The Contractor's Staff, engaged within the boundaries of the Premises shall comply with such rules, regulations and requirements (including those relating to security arrangements) as may be in force from time to time for the conduct of personnel when at or outside the Premises.

7.7 The Customer may require the Contractor to ensure that any person employed in the provision of the Services has undertaken a Criminal Records Bureau check as per the Staff Vetting Procedures.

8 Assignment and sub-contracting

8.1 The Contractor shall not without the written consent of the Customer assign, sub-contract, novate or in any way dispose of the benefit and/ or the burden of the Agreement or any part of the Agreement. The Customer may, in the granting of such consent, provide for additional terms and conditions relating to such assignment, sub-contract, novation or disposal. The Contractor shall be responsible for the acts and omissions of its sub-contractors as though those acts and omissions were its own.

8.2 If the Contractor enters into a sub-contract for the purpose of performing its obligations under the Agreement, it shall ensure that a provision is included in such sub-contract which requires payment to be made of all sums due by the Contractor to the sub-contractor within a specified period not exceeding 30 days from the receipt of a valid invoice.

8.3 If the Customer has consented to the placing of sub-contracts, the Contractor shall, at the request of the Customer, send copies of each sub-contract, to the Customer as soon as is reasonably practicable.

8.4 The Customer may assign, novate, or otherwise dispose of its rights and obligations under the Agreement without the consent of the Contractor provided that such assignment, novation or disposal shall not increase the burden of the Contractor's obligations under the Agreement.

9 Intellectual Property Rights

9.1 Intellectual Property ("IP") means all forms of intellectual property, including, without limitation, property in and rights under copyright, patents, conceptual solutions, circuit layout rights, performance rights, design rights, designs, database rights, trade names, trademarks, service marks, methodologies, ideas, processes, methods, tools and know-how and entitlement to make application for formal (or otherwise enhanced) rights of any such nature

9.2 IP and rights to IP owned by either Party on the date of the Agreement or created outside the terms of this Agreement ("Background IP") shall remain the property of that Party.

9.3 All intellectual property rights in any materials provided by the Customer to the Contractor for the purposes of this Agreement shall remain the property of the Customer but the Customer hereby grants the Contractor a royalty-free, non-exclusive and non-transferable licence to use such materials as required until termination or expiry of the Agreement for the sole purpose of enabling the Contractor to perform its obligations under the Agreement.

9.4 All intellectual property rights in any materials created or developed by the Contractor pursuant to the Agreement or arising as a result of the provision of the Services shall vest in the Customer. If, and to the extent, that any intellectual property rights in such materials vest in the Contractor by operation of law, the Contractor hereby assigns to the Customer by way of a present assignment of future rights that shall take place immediately on the coming into existence of any such intellectual property rights all its intellectual property rights in such materials (with full title guarantee and free from all third party rights).

9.5 The Contractor hereby grants the Customer:

9.5.1 a perpetual, royalty-free, irrevocable, non-exclusive licence (with a right to sub-license) to use all intellectual property rights in the materials created or developed pursuant to the Agreement and any intellectual property rights arising as a result of the provision of the Services; and

9.5.2 a perpetual, royalty-free, irrevocable and non-exclusive licence (with a right to sub-license) to use:

a) any intellectual property rights vested in or licensed to the Contractor on the date of the Agreement; and

b) any intellectual property rights created during the Term but which are neither created or developed pursuant to the Agreement nor arise as a result of the provision of the Services,

including any modifications to or derivative versions of any such intellectual property rights, which the Customer reasonably requires in order to exercise its rights and take the benefit of the Agreement including the Services provided.

9.6 Subject to Clause 9.8, the Contractor shall indemnify, and keep indemnified, the Customer 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 Customer as a result of or in connection with any claim made against the Customer 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 the Contractor its Staff, agents or sub-contractors.

9.7 The Customer shall promptly notify the Contractor of any infringement claim made against it relating to any Services and, subject to any statutory obligation requiring the Customer to respond, shall permit the Contractor to have the right, at its sole discretion to assume, defend, settle or otherwise dispose of such claim. The Customer shall give the Contractor such assistance as it may reasonably require to dispose of the claim and shall not make any statement which might be prejudicial to the settlement or defence of the claim.

9.8 The Contractor may in the performance of the Services use Open Source Software and application tools. Subject to Clause 8, if the Contractor enters into a sub-contract for the purpose of performing its obligations under the Agreement, the Sub- contractor gives no warranty or indemnity that the possession and/or use of such software and application tools or any part thereof is not an infringement of any third party rights or any other rights and the Contractor does not give any warranty or indemnity that no third party has any right, title or interest therein.

9.9 Furthermore, whilst the Contractor shall use all reasonable endeavours to ensure that any such Open Source Software and application tools and any other tools used in the provision of the penetration testing services (whether open source or otherwise) are appropriate, the Contractor shall not be liable for any adverse effects reasonably unknown to the Contractor and in relation to any software and application tools which have published uses, the Contractor shall not be liable for any use or consequences of use that are unpublished or otherwise reasonably unknown to the Contractor.

10 Governance and Records

10.1 The Contractor shall:

10.1.1 attend progress meetings with the Customer at the frequency and times specified by the Customer and shall ensure that its representatives are suitably qualified to attend such meetings; and

10.1.2 submit progress reports to the Customer at the times and in the format specified by the Customer.

10.2 The Contractor shall keep and maintain until 6 years after the end of the Agreement, or as long a period as may be agreed between the Parties, full and accurate records of the Agreement including the Services supplied under it and all payments made by the Customer. The Contractor shall on request afford the Customer or the Customer's representatives such access to those records as may be reasonably requested by the Customer in connection with the Agreement.

11 Confidentiality, Transparency and Publicity

11.1 Subject to clause 11.2, each Party shall:

11.1.1 treat all Confidential Information it receives as confidential, safeguard it accordingly and not disclose it to any other person without the prior written permission of the disclosing Party; and

11.1.2 not use or exploit the disclosing Party's Confidential Information in any way except for the purposes anticipated under the Agreement.

11.2 Notwithstanding clause 11.1, a Party may disclose Confidential Information which it receives from the other Party:

11.2.1 where disclosure is required by applicable law or by a court of competent jurisdiction;

11.2.2 to its auditors or for the purposes of regulatory requirements;

11.2.3 on a confidential basis, to its professional advisers;

11.2.4 to the Serious Fraud Office where the Party has reasonable grounds to believe that the other Party is involved in activity that may constitute a criminal offence under the Bribery Act 2010;

11.2.5 where the receiving Party is the Contractor, to the Staff on a need to know basis to enable performance of the Contractor's obligations under the Agreement provided that the Contractor shall procure that any Staff to whom it discloses Confidential Information pursuant to this clause 11.2.5 shall observe the Contractor's confidentiality obligations under the Agreement; and

11.2.6 where the receiving Party is the Customer:

a) on a confidential basis to the employees, agents, consultants and contractors of the Customer;

b) on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company to

which the Customer transfers or proposes to transfer all or any part of its business;

c) to the extent that the Customer (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions; or

d) in accordance with clause 12.

and for the purposes of the foregoing, references to disclosure on a confidential basis shall mean disclosure subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the Customer under this clause 11.

11.3 The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of the Agreement is not Confidential Information and the Contractor hereby gives its consent for the Customer to publish this Agreement in its entirety to the general public (but with any information that is exempt from disclosure in accordance with the FOIA redacted) including any changes to the Agreement agreed from time to time. The Customer may consult with the Contractor to inform its decision regarding any redactions but shall have the final decision in its absolute discretion whether any of the content of the Agreement is exempt from disclosure in accordance with the provisions of the FOIA.

11.4 The Contractor shall not, and shall take reasonable steps to ensure that the Staff shall not, make any press announcement or publicise the Agreement or any part of the Agreement in any way, except with the prior written consent of the Customer.

12 Freedom of Information

12.1 The Contractor acknowledges that the Customer is subject to the requirements of the FOIA and the Environmental Information Regulations 2004 and shall and procure that any sub-contractor shall:

12.1.1 provide all necessary assistance and cooperation as reasonably requested by the Customer to enable the Customer to comply with its obligations under the FOIA and the Environmental Information Regulations 2004;

12.1.2 transfer to the Customer all Requests for Information relating to this Agreement that it receives as soon as practicable and in any event within 2 Working Days of receipt;

12.1.3 provide the Customer with a copy of all Information belonging to the Customer requested in the Request for Information which is in its

possession or control in the form that the Customer requires within 5 Working Days (or such other period as the Customer may reasonably specify) of the Customer's request for such Information; and

12.1.4 not respond directly to a Request for Information unless authorised in writing to do so by the Customer.

12.2 The Contractor acknowledges that the Customer may be required under the FOIA and the Environmental Information Regulations 2004 to disclose Information concerning the Contractor or the Services (including commercially sensitive information) without consulting or obtaining consent from the Contractor. In these circumstances the Customer shall, in accordance with any relevant guidance issued under the FOIA, take reasonable steps, where appropriate, to give the Contractor advance notice, or failing that, to draw the disclosure to the Contractor's attention after any such disclosure.

12.3 Notwithstanding any other provision in the Agreement, the Customer shall be responsible for determining in its absolute discretion whether any Information relating to the Contractor or the Services is exempt from disclosure in accordance with the FOIA and/or the Environmental Information Regulations 2004.

13 Protection of Personal Data and Security of Data

13.1 The Contractor shall, and shall procure that all Staff shall, comply with any notification requirements under the DPA and both Parties shall duly observe all their obligations under the DPA which arise in connection with the Agreement.

13.2 Notwithstanding the general obligation in clause 13.1, where the Contractor is processing Personal Data for the Customer as a data processor (as defined by the DPA) the Contractor shall:

13.2.1 process the Personal Data only in accordance with instructions from the Customer (which may be specific instructions or instructions of a general nature) as set out in this Contract or as otherwise notified by the Customer;

13.2.2 comply with all applicable laws;

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

13.2.4 obtain prior written consent from the Customer in order to transfer the Persona Data to any sub-contractor for the provision of the Services;

13.2.5 not cause or permit the Personal Data to be transferred outside of the European Economic Area without the prior consent of the Customer;

13.2.6 not disclose Personal Data to any third parties in any circumstances other than with the written consent of the Customer or in compliance with a legal obligation imposed upon the Customer;

13.2.7 ensure that it has in place appropriate technical and organisational measures to ensure the security of the Personal Data (and to guard against unauthorised or unlawful processing of the Personal Data and against accidental loss or destruction of, or damage to, the Personal Data), as required under the Seventh Data Protection Principle in Schedule 1 to the DPA;

13.2.8 provide the Customer with such information as the Customer may reasonably request to satisfy itself that the Contractor is complying with its obligations under the DPA;

13.2.9 promptly notify the Customer of:

a) any breach of the security requirements of the Customer as referred to in clause 13.3; and

b) any complaint or request for personal data; and

13.2.10 ensure that it does not knowingly or negligently do or omit to do anything which places the Customer in breach of the Customer's obligations under the DPA.

13.3 When handling Customer data (whether or not Personal Data), the Contractor shall ensure the security of the data is maintained in line with the security requirements of the Customer as notified to the Contractor from time to time.

13.4 The Contractor shall fully indemnify the Customer against the costs of dealing with any claims made in respect of any information subject to the DPA, which claims would not have arisen but for some act, omission or negligence on the part of the Contractor, its sub-contractors, agent or Staff.

13.5 The Contractor shall be liable for, and shall indemnify the Customer against all actions, suits, claims, demands, losses, charges, costs and expenses suffered or incurred by the Customer and/or any third party arising from and/or in connection with any Breach of Security or attempted Breach of

Security (to the extent that such actions, suits, claims, demands, losses, charges, costs and expenses were not caused by any act or omission by the Customer).

13.6 The provisions of this clause shall apply during the term of the agreement and indefinitely after its expiry or termination.

14 Liability and Insurance

14.1 The Contractor shall not be responsible for any injury, loss, damage, cost or expense suffered by the Customer if and to the extent that it is caused by the negligence or wilful misconduct of the Customer or by breach by the Customer of its obligations under the Agreement.

14.2 Subject always to clauses 14.1, 14.3 and 14.4:

14.2.1 the aggregate liability of the Contractor in respect of all defaults, claims, losses or damages howsoever caused, whether arising from breach of the Agreement, the supply or failure to supply of the Services, misrepresentation (whether tortuous or statutory), tort (including negligence), breach of statutory duty or otherwise shall in no event exceed a sum equal to 125% of the Charges paid or payable to the Contractor; and

14.2.2 except in the case of claims arising under clauses 9.6 and 18.4, in no event shall the Contractor be liable to the Customer for any:

a) loss of profits;

b) loss of business;

c) loss of revenue;

d) loss of or damage to goodwill;

e) loss of savings (whether anticipated or otherwise);

f) any damage to any hardware, software or data stored or used in connection with the services including the cost of repairing, replacing or recovering the same;

g) any unauthorised or third party access to, or any alteration of, any e-mail or other transmission, material, content or data sent or received, or which should have been sent or received, by Customer in relation to the services or any loss or damage suffered or incurred by Customer caused by any performance or communication failure, operational delay, error, omission,

interruption, deletion, defect, computer virus or security breach arising in connection with the services;

h) any pre-existing known or unknown faults, malfunctions, damage, corruption, bugs viruses or similar destructive programs or code, of any other deficiencies in any software or computer system of the Customer which are discovered, revealed or manifested in the course of or pursuant to the provision of the Services;

i) loss of connectivity, degradation of network bandwidth or loss of access to any systems, programs, data or networks, unintentional transmission of viruses or other harmful components whatsoever and howsoever arising out of or in connection with this Agreement; and/or

j) any indirect, special or consequential loss or damage.

14.3 Nothing in the Agreement shall be construed to limit or exclude either Party's liability for:

14.3.1 death or personal injury caused by its negligence or that of its Staff;

14.3.2 fraud or fraudulent misrepresentation by it or that of its Staff; or

14.3.3 any other matter which, by law, may not be excluded or limited.

14.4 The Contractor’s liability under the indemnity in clause 9.6 and 18.4 shall be unlimited.

14.5 The Contractor shall hold:

a) Employer’s liability insurance providing an adequate level of cover in respect of all risks which may be incurred by the Contractor;

b) Public liability with the minimum cover per claim of £ 1 million pounds (£ 1, 000,000);

c) Professional indemnity with the minimum cover per claim of £ [one] million pounds (£ 1, 000,000);

or any sum as required by Law unless otherwise agreed with the Customer in writing. Such insurance shall be maintained for the duration of the Term and for a minimum of six (6) years following the expiration or earlier termination of the Agreement.

15 Force Majeure

15.1 Neither Party shall have any liability under or be deemed to be in breach of the Agreement for any delays or failures in performance of the Agreement which result from circumstances beyond the reasonable control of the Contractor. Each Party shall promptly notify the other Party in writing, using the most expeditious method of delivery, when such circumstances cause a delay or failure in performance, an estimate of the length of time delay or failure shall continue and when such circumstances cease to cause delay or failure in performance. If such circumstances continue for a continuous period of more than 30 days, either Party may terminate the Agreement by written notice to the other Party.

15.2 Any failure by the Contractor in performing its obligations under the Agreement which results from any failure or delay by an agent, sub-contractor or supplier shall be regarded as due to Force Majeure only if that agent, sub-contractor or supplier is itself impeded by Force Majeure from complying with an obligation to the Contractor.

16 Termination

16.1 The Customer may terminate the Agreement at any time by notice in writing to the Contractor to take effect on any date falling at least 1 month (or, if the Agreement is less than 3 months in duration, at least 10 Working Days) later than the date of service of the relevant notice.

16.2 Without prejudice to any other right or remedy it might have, the Customer may terminate the Agreement by written notice to the Contractor with immediate effect if the Contractor:

16.2.1 (without prejudice to clause 16.2.5), is in material breach of any obligation under the Agreement which is not capable of remedy;

16.2.2 repeatedly breaches any of the terms and conditions of the Agreement in such a manner as to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms and conditions of the Agreement;

16.2.3 is in material breach of any obligation which is capable of remedy, and that breach is not remedied within 30 days of the Contractor receiving notice specifying the breach and requiring it to be remedied;

16.2.4 undergoes a change of control within the meaning of section 416 of the Income and Corporation Taxes Act 1988;

16.2.5 breaches any of the provisions of clauses 7.2, 11, 12, 13 and 17; or

16.2.6 becomes insolvent, or if an order is made or a resolution is passed for the winding up of the Contractor (other than voluntarily for the purpose of solvent amalgamation or reconstruction), or if an administrator or administrative receiver is appointed in respect of the whole or any part of the Contractor's assets or business, or if the Contractor makes any composition with its creditors or takes or suffers any similar or analogous action (to any of the actions detailed in this clause 16.2.6) in consequence of debt in any jurisdiction.

16.3 The Contractor shall notify the Customer as soon as practicable of any change of control as referred to in clause 16.2.4 or any potential such change of control.

16.4 The Contractor may terminate the Agreement by written notice to the Customer if the Customer has not paid any undisputed amounts within 90 days of them falling due.

16.5 Termination or expiry of the Agreement shall be without prejudice to the rights of either Party accrued prior to termination or expiry and shall not affect the continuing rights of the Parties under this clause and clauses 2, 3.2, 6.1, 6.2, 6.6, 6.7, 7, 9, 10.2, 11, 12, 13, 14, 16.6, 17.4, 18.4, 19 and 20.8 or any other provision of the Agreement that either expressly or by implication has effect after termination.

16.6 Upon termination or expiry of the Agreement, the Contractor shall:

16.6.1 give all reasonable assistance to the Customer and any incoming Contractor of the Services; and

16.6.2 return all requested documents, information and data to the Customer as soon as reasonably practicable.

17 Compliance and Customer Consents

Compliance

17.1 The Contractor shall promptly notify the Customer of any health and safety hazards which may arise in connection with the performance of its obligations under the Agreement. The Customer shall promptly notify the Contractor of any health and safety hazards which may exist or arise at the Customer's premises and which may affect the Contractor in the performance of its obligations under the Agreement.

17.2 The Contractor shall:

17.2.1 comply with all the Customer's health and safety measures while on the Customer's premises; and

17.2.2 notify the Customer immediately of any incident occurring in the performance of its obligations under the Agreement on the Customer's premises where that incident causes any personal injury or damage to property which could give rise to personal injury.

17.3 The Contractor shall:

17.3.1 perform its obligations under the Agreement in accordance with all applicable equality Law and the Customer's equality and diversity policy as provided to the Contractor from time to time; and

17.3.2 take all reasonable steps to secure the observance of clause 17.3.1 by all Staff.

17.4 The Contractor shall supply the Services in accordance with the Customer's environmental policy as provided to the Contractor from time to time.

17.5 The Contractor shall comply with, and shall ensure that its Staff shall comply with, the provisions of:

17.5.1 the Official Secrets Acts 1911 to 1989; and

17.5.2 section 182 of the Finance Act 1989.

Customer Consents for Penetration Testing

17.6 For the purposes of the UK Computer Misuse Act 1990 (or any statutory modification or re-enactment), Customer consents to the Contractor accessing and assessing its information technology systems and networks (including without limitation any programs or data held on such systems and networks) to enable the Contractor to provide the Services.

17.7 Customer warrants to the Contractor that:

(a) it has obtained all necessary third party consents and licences to permit the Contractor to perform the penetration testing services (including without limitation any necessary consents and licences for PA to access and assess the Customer's information technology systems and networks and programs or data held on such systems and networks);

(b) the Contractor's access to and assessment of the Customer's information technology systems and networks (including without limitation any programs or data held on such systems and networks) will not infringe the rights of any third party; and

(c) it will not act in any way which may result in the Contractor incurring any liability under the UK Computer Misuse Act 1990 (or any statutory modifications or re-enactments).

17.8 Customer hereby indemnifies and shall keep the Contractor indemnified (on demand) against all costs, claims, liabilities and expenses incurred by the Contractor, its officers, employees, affiliates, sub-contractors and agents as a result of or in connection with any breach of the warranties in Clause 17.7 above.

18 Prevention of Fraud, Corruption and Bribery

18.1 The Contractor represents and warrants that neither it, nor to the best of its knowledge any Staff, have at any time prior to the Commencement Date:

18.1.1 Committed a Prohibited Act or been formally notified that it is subject to an investigation or prosecution which relates to an alleged Prohibited Act and/or

18.1.2 Been listed by any government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in government procurement programmes or contracts on the grounds of a Prohibited Act.

18.2 The Contractor shall not during the Term:

18.2.1 commit a Prohibited Act; and/or

18.2.2 do or suffer anything to be done which would cause the Customer or any of its employees, consultants, contractors, sub-contractors or agents to contravene any of the Relevant Requirements or otherwise incur any liability in relation to the Relevant Requirements.

18.3 The Contractor shall, during the Term establish, maintain and enforce, and require that its Sub-Contractors establish, maintain and enforce, policies and procedures which are adequate to ensure compliance with the Relevant Requirements and prevent the occurrence of a Prohibited Act; and shall notify the Customer immediately if it has reason to suspect that any breach of clauses 18.1 and/or 18.2 has occurred or is occurring or is likely to occur.

18.4 If the Contractor or the Staff engages in conduct prohibited by clause 18.1 or commits fraud in relation to the Agreement or any other contract with the Crown (including the Customer) the Customer may:

18.4.1 terminate the Agreement and recover from the Contractor the amount of any loss suffered by the Customer resulting from the termination, including the cost reasonably incurred by the Customer

of making other arrangements for the supply of the Services and any additional expenditure incurred by the Customer throughout the remainder of the Agreement; or

18.4.2 recover in full from the Contractor any other loss sustained by the Customer in consequence of any breach of this clause.

19 Dispute Resolution

19.1 The Parties shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with the Agreement within 20 Working Days of either Party notifying the other of the dispute and such efforts shall involve the escalation of the dispute to an appropriately senior representative of each Party.

19.2 If the dispute cannot be resolved by the Parties within one month of being escalated as referred to in clause 19.1, the dispute may by agreement between the Parties be referred to a neutral adviser or mediator (the "Mediator") chosen by agreement between the Parties. All negotiations connected with the dispute shall be conducted in confidence and without prejudice to the rights of the Parties in any further proceedings.

19.3 If the Parties fail to appoint a Mediator within one month 20 Working Days of the agreement to refer to a Mediator, either Party shall apply to the Centre for Effective Dispute Resolution to appoint a Mediator.

19.4 If the Parties fail to enter into a written agreement resolving the dispute within one month of the Mediator being appointed, or such longer period as may be agreed by the Parties, either Party may refer the dispute to Court.

19.5 The commencement of mediation shall not prevent the parties commencing or continuing court or arbitration proceedings in relation to the dispute.

20 General

20.1 Each of the Parties represents and warrants to the other that it has full capacity and authority, and all necessary consents, licences and permissions to enter into and perform its obligations under the Agreement, and that the Agreement is executed by its duly authorised representative.

20.2 A person who is not a party to the Agreement shall have no right to enforce any of its provisions which, expressly or by implication, confer a benefit on him, without the prior written agreement of the Parties. This clause does not affect any right or remedy of any person which exists or is available apart from the Contracts (Rights of Third Parties) Act 1999 and does not apply to the Crown.

20.3 The Agreement cannot be varied except in writing signed by a duly authorised representative of both the Parties.

20.4 In the event that the Contractor is unable to accept the variation to the Specification or where the Parties are unable to agree a change to the Contract Price, the Customer may:

20.4.1 allow the Contractor to fulfil its obligations under the Agreement without the variation to the Specification;

20.4.2 terminate the Contract with immediate effect, except where the Contractor has already provided all or part of the Services or where the Contractor can show evidence of substantial work being carried out to fulfil the requirement of the Specification, and in such case the Parties shall attempt to agree upon a resolution to the matter. Where a resolution cannot be reached, the matter shall be dealt with under the Dispute Resolution procedure detailed at clause 19.

20.5 The Agreement contains the whole agreement between the Parties and supersedes and replaces any prior written or oral agreements, representations or understandings between them. The Parties confirm that they have not entered into the Agreement on the basis of any representation that is not expressly incorporated into the Agreement. Nothing in this clause shall exclude liability for fraud or fraudulent misrepresentation.

20.6 Any waiver or relaxation either partly, or wholly of any of the terms and conditions of the Agreement shall be valid only if it is communicated to the other Party in writing and expressly stated to be a waiver. A waiver of any right or remedy arising from a breach of contract shall not constitute a waiver of any right or remedy arising from any other breach of the Agreement.

20.7 The Agreement shall not constitute or imply any partnership, joint venture, agency, fiduciary relationship or other relationship between the Parties other than the contractual relationship expressly provided for in the Agreement. Neither Party shall have, nor represent that it has, any authority to make any commitments on the other Party's behalf.

20.8 Except as otherwise expressly provided by the Agreement, all remedies available to either Party for breach of the Agreement (whether under the Agreement, statute or common law) are cumulative and may be exercised concurrently or separately, and the exercise of one remedy shall not be deemed an election of such remedy to the exclusion of other remedies.

20.9 If any provision of the Agreement is prohibited by law or judged by a court to be unlawful, void or unenforceable, the provision shall, to the extent required, be severed from the Agreement and rendered ineffective as far as possible without modifying the remaining provisions of the Agreement, and shall not in

any way affect any other circumstances of or the validity or enforcement of the Agreement.

20.10 The Contractor shall take appropriate steps to ensure that neither the Contractor nor any Staff is placed in a position where, in the reasonable opinion of the Customer, there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the Contractor and the duties owed to the Customer under the provisions of the Agreement. The Contractor will disclose to the Customer full particulars of any such conflict of interest which may arise.

20.11 The Customer reserves the right to terminate the Agreement immediately by notice in writing and/or to take such other steps it deems necessary where, in the reasonable opinion of the Customer, there is or may be an actual conflict, or potential conflict between the pecuniary or personal interest of the Contractor and the duties owed to the Customer pursuant to this clause shall not prejudice or affect any right of action or remedy which shall have accrued or shall thereafter accrue to the Customer.

20.12 The Agreement constitutes the entire contract between the Parties in respect of the matters dealt with therein. The Agreement supersedes all prior negotiations between the Parties and all representations and undertakings made by one Party to the other, whether written or oral, except that this clause shall not exclude liability in respect of any Fraud or fraudulent misrepresentation.

21 Notices

21.1 Except as otherwise expressly provided in the Agreement, no notice or other communication from one Party to the other shall have any validity under the Agreement unless made in writing by or on behalf of the Party concerned.

21.2 Any notice or other communication which is to be given by either Party to the other shall be given by letter (sent by hand, first class post, recorded delivery or special delivery), or by facsimile transmission or electronic mail (confirmed in either case by letter), Such letters shall be addressed to the other Party in the manner referred to in clause 21.3. Provided the relevant communication is not returned as undelivered, the notice or communication shall be deemed to have been given 2 Working Days after the day on which the letter was posted, or 4 hours, in the case of electronic mail or facsimile transmission or sooner where the other Party acknowledges receipt of such letters, facsimile transmission or item of electronic mail.

21.3 For the purposes of clause 21.2, the address of each Party shall be:

21.3.1 For the Customer:

[Address:] Care Quality Commission, 151 Buckingham Palace Road,

London, SW1W 9SZ

For the attention of: [redacted]

[Tel:] [redacted]

[redacted]

21.3.2 For the Contractor: 7 Safe

[Address:]

For the attention of: [redacted]

[Tel:]

[Email:] [redacted]

[Fax:]

21.4 Either Party may change its address for service by serving a notice in accordance with this clause.

21.5 Notices under clauses 15 (Force Majeure) and 16 (Termination) may be served by email only if the original notice is then sent to the recipient by personal delivery or recorded delivery in the manner set out in clause 21.1.

22 Governing Law and Jurisdiction

The validity, construction and performance of the Agreement, and all contractual and non-contractual matters arising out of it, shall be governed by English law and shall be subject to the exclusive jurisdiction of the English courts to which the Parties submit.

Schedule 1 – Specification

Healthwatch CRM - Penetration testing high level objectives

Testing is required for three systems:

1. CiviCRM – We have a host site, and have rolled out 87 instances across our network
2. Web in a box (password protected demo site for local Healthwatch)
3. Healthwatch public website (www.healthwatch.co.uk)

We require the following testing:

1) Blackbox testing (no details provided to pen testing team):

1.1) Footprinting phase:

- Pen testing team to search the internet, querying various public repositories (whois databases, domain registrars, Usenet groups, mailing lists, etc.) for any useful system information

- Can include social engineering (i.e. checking social networks etc. for public system data but perhaps we do not need this?)

2) Whitebox testing

This term is used when the Pen testing team are given information about the servers and application.

1.2) Scanning and Enumeration:

Based on information found in footprinting, pen test team should scan:

1.2.1) Infrastructure:

open / filtered ports found,

services running on these ports,

mapping router / firewall rules,

identifying the operating system details

network path discovery,

1.2.2) Application level:

Parameter injection, Cross-site scripting, Directory traversal, SQL injection, Buffer overflow, DoS, Format String (there may be more elements to test for and we should confirm).

We should confirm what automated tools and manual methods will be used.

1.3 API testing

High level testing to identify access only.

Vulnerability status should then be provided to us to review.

Contract Commencement/Term

- CRM Testing to take place in August 2017 – September 2018
- Website Testing to take place between January 2018 – March 2018

Start Date	Expiry Date	Extension (If Applicable)
25th August 2017	31st March 2018	Possible extension of up to 12 months following confirmation from the Customer. To be executed by a Contract Change Note.

Schedule 2 – Charges

Project break down:

Web Application Component	
Blackbox Testing of www.healthwatch.co.uk (offsite):	[redacted]
Blackbox Testing of www.healthwatchwib.co.uk (offsite):	
Blackbox Testing of SharePoint hub (offsite):	
Reporting for Blackbox Assessment: including Peer Review and Quality Assurance:	
Greybox Testing of www.healthwatch.co.uk (offsite):	
Reporting for Greybox Assessment: including Peer Review and Quality Assurance:	
API Assessment (based on an estimate of 20 APIs) (offsite):	
Reporting for API Assessment: including Peer Review and Quality Assurance:	

The Quotation

Total Project Fee:	£17,737.50 + VAT
Additional Costs (where applicable):	Rates are subject to 7Safe's expenses (Please Refer to Appendix B: 7Safe Working Policies).

Additional notes

This proposal is priced as a fixed fee based on a total project which includes our estimate of [redacted] of testing. Should the project not be completed within the [redacted] 7Safe reserves the right to invoice any additional days as an additional project.

The total cost for delivery of the Services will be £17,737.50 (ex VAT)

Payments to be made upon successful delivery of the contract deliverables within schedule 1.

Schedule 3 – 7Safe Tender Response

Reference 22404v2

Schedule 4 – Security Requirement, Policy and Plan

INTERPRETATION AND DEFINITION

For the purposes of this Schedule 8, unless the context otherwise requires the following provisions shall have the meanings given to them below:

"Breach of Security" means the occurrence of unauthorised access to or use of the Premises, the Premises, the Services, the Contractor System, or any ICT or data (including Authority Data) used by the Authority or the Contractor in connection with the Contract.

"Contractor Equipment" means the hardware, computer and telecoms devices and equipment supplied by the Contractor or its Sub-Contractor (but not hired, leased or loaned from the Authority) for the provision of the Services;

"Contractor Software" means software which is proprietary to the Contractor, including software which is or will be used by the Contractor for the purposes of providing the Services and which is specified as such in Schedule 6.

"ICT" means Information Communications Technology and includes a diverse set of technological tools and resources used to communicate, and to create, disseminate, store and manage information, including computers, the Internet, broadcasting technologies (radio and television), and telephony.

"Protectively Marked" shall have the meaning as set out in the Security Policy Framework.

"Security Plan" means the Contractor's security plan prepared pursuant to paragraph 3 an outline of which is set out in an Appendix to this Schedule 8.

"Software" means Specially Written Software, Contractor Software and Third Party Software.

"Specially Written Software" means any software created by the Contractor (or by a third party on behalf of the Contractor) specifically for the purposes of this Contract.

"Third Party Software" means software which is proprietary to any third party which is or will be used by the Contractor for the purposes of providing the Services including the software and which is specified as such in Schedule 6.

1. INTRODUCTION

This Schedule 7 covers:

1.1 principles of security for the Contractor System, derived from the Security Policy Framework, including without limitation principles of physical and information security;

1.2 wider aspects of security relating to the Services;

1.3 the creation of the Security Plan;

1.4 audit and testing of the Security Plan; and

1.5 breaches of security.

2. PRINCIPLES OF SECURITY

2.1 The Contractor acknowledges that the Authority places great emphasis on confidentiality, integrity and availability of information and consequently on the security of the Premises and the security for the Contractor System. The Contractor also acknowledges the confidentiality of Authority Data.

2.2 The Contractor shall be responsible for the security of the Contractor System and shall at all times provide a level of security which:

2.2.1 is in accordance with Good Industry Practice and Law;

2.2.2 complies with Security Policy Framework; and

2.2.3 meets any specific security threats to the Contractor System.

2.3 Without limiting paragraph 2.2, the Contractor shall at all times ensure that the level of security employed in the provision of the Services is appropriate to maintain the following at acceptable risk levels (to be defined by the Authority):

2.3.1 loss of integrity of Authority Data;

2.3.2 loss of confidentiality of Authority Data;

2.3.3 unauthorised access to, use of, or interference with Authority Data by any person or organisation;

2.3.4 unauthorised access to network elements, buildings, the Premises, and tools used by the Contractor in the provision of the Services;

2.3.5 use of the Contractor System or Services by any third party in order to gain unauthorised access to any computer resource or Authority Data; and

2.3.6 loss of availability of Authority Data due to any failure or compromise of the Services.

2.3.7 processing and storage of authority data within the UK or by exception within the EEA. Any processing outside of the UK must be subject to specific approval by the Authority.

3. SECURITY PLAN

3.1 The Contractor shall develop, implement and maintain a Security Plan to apply during the Contract Period (and after the end of the term as applicable) which will be approved by the Authority, tested, periodically updated and audited in accordance with this Schedule 7.

3.2 A draft Security Plan provided by the Contractor as part of its bid is set out herein.

3.3 Prior to the Commencement Date the Contractor will deliver to the Authority for approval the final Security Plan which will be based on the draft Security Plan set out herein.

3.4 If the Security Plan is approved by the Authority it will be adopted immediately. If the Security Plan is not approved by the Authority the Contractor shall amend it within 10 Working Days of a notice of non-approval from the Authority and re-submit to the Authority for approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the Security Plan following its resubmission, the matter will be resolved in accordance with clause I2 (Dispute Resolution). No approval to be given by the Authority pursuant to this paragraph 3.4 may be unreasonably withheld or delayed. However any failure to approve the Security Plan on the grounds that it does not comply with the requirements set out in paragraphs 3.1 to 3.4 shall be deemed to be reasonable.

3.5 The Security Plan will set out the security measures to be implemented and maintained by the Contractor in relation to all aspects of the Services and all processes associated with the delivery of the Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with:

3.5.1 the provisions of this Schedule 7;

3.5.2 the provisions of Schedule 1 relating to security;

3.5.3 the Information Assurance Standards;

3.5.4 the data protection compliance guidance produced by the Authority;

3.5.5 the minimum set of security measures and standards required where the system will be handling Protectively Marked or sensitive information, as determined by the Security Policy Framework;

3.5.6 any other extant national information security requirements and guidance, as provided by the Authority's IT security officers; and

3.5.7 appropriate ICT standards for technical countermeasures which are included in the Contractor System.

3.6 The references to Quality Standards, guidance and policies set out in this Schedule shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such Quality Standards, guidance and policies, from time to time.

3.7 If there is any inconsistency in the provisions of the above standards, guidance and policies, the Contractor should notify the Authorised Representative of such inconsistency immediately upon becoming aware of the same, and the Authorised Representative shall, as soon as practicable, advise the Contractor which provision the Contractor shall be required to comply with.

3.8 The Security Plan will be structured in accordance with ISO/IEC27002 and ISO/IEC27001 or other equivalent policy or procedure, cross-referencing if necessary to other schedules of the Contract which cover specific areas included within that standard.

3.9 The Security Plan shall not reference any other documents which are not either in the possession of the Authority or otherwise specified in this Schedule 7.

4. AMENDMENT AND REVISION

4.1 The Security Plan will be fully reviewed and updated by the Contractor annually or from time to time to reflect:

4.1.1 emerging changes in Good Industry Practice;

4.1.2 any change or proposed change to the Contractor System, the Services and/or associated processes;

4.1.3 any new perceived or changed threats to the Contractor System;

4.1.4 changes to security policies introduced Government-wide or by the Authority; and/or

4.1.5 a reasonable request by the Authority.

4.2 The Contractor will provide the Authority with the results of such reviews as soon as reasonably practicable after their completion and amend the Security Plan at no additional cost to the Authority.

4.3 Any change or amendment which the Contractor proposes to make to the Security Plan (as a result of an Authority request or change to Schedule 1 or otherwise) shall be subject to a CCN and shall not be implemented until Approved.

5. AUDIT AND TESTING

5.1 The Contractor shall conduct tests of the processes and countermeasures contained in the Security Plan ("Security Tests") on an annual basis or as otherwise agreed by the Parties. The date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority.

5.2 The Authority shall be entitled to send a representative to witness the conduct of the Security Tests. The Contractor shall provide the Authority with the results of such tests (in an Approved form) as soon as practicable after completion of each Security Test.

5.3 Without prejudice to any other right of audit or access granted to the Authority pursuant to the Contract, the Authority shall be entitled at any time and without giving notice to the Contractor to carry out such tests (including penetration tests) as it may deem necessary in relation to the Security Plan and the Contractor's compliance with and implementation of the Security Plan. The Authority may notify the Contractor of the results of such tests after completion of each such test. Security Tests shall be designed and implemented so as to minimise the impact on the delivery of the Services.

5.4 Where any Security Test carried out pursuant to paragraphs 5.2 or 5.3 reveals any actual or potential security failure or weaknesses, the Contractor shall promptly notify the Authority of any changes to the Security Plan (and the implementation thereof) which the Contractor proposes to make in order to correct such failure or weakness. Subject to Approval in accordance with paragraph 4.3, the Contractor shall implement such changes to the Security Plan in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the Security Plan to address a non-compliance with the Security Policy Framework or security requirements, the change to the Security Plan shall be at no additional cost to the Authority. For the purposes of this paragraph, a weakness means a vulnerability in security and a potential security failure means a possible breach of the Security Plan or security requirements.

6. BREACH OF SECURITY

6.1 Either Party shall notify the other immediately upon becoming aware of any Breach of Security including, but not limited to an actual, potential or attempted breach, or threat to, the Security Plan.

6.2 Upon becoming aware of any of the circumstances referred to in paragraph 6.1, the Contractor shall immediately take all reasonable steps necessary to:

6.2.1 remedy such breach or protect the Contractor System against any such potential or attempted breach or threat; and

6.2.2 prevent an equivalent breach in the future;

6.2.3 collect, preserve and protect all available audit data relating to the incident and make it available on request to the Authority;

6.2.4 investigate the incident and produce a detailed report for the Authority within 5 working days of the discovery of the incident.

6.3 Such steps shall include any action or changes reasonably required by the Authority. If such action is taken in response to a breach that is determined by the Authority acting reasonably not to be covered by the obligations of the Contractor under the Contract, then the Contractor shall be entitled to refer the matter to the CCN procedure set out in Schedule 3.

6.4 The Contractor shall as soon as reasonably practicable provide to the Authority full details (using such reporting mechanism as may be specified by the Authority from time to time) of such actual, potential or attempted breach and of the steps taken in respect thereof.

7. CONTRACT EXIT – SECURITY REQUIREMENTS

7.1 On termination of the contract, either via early termination or completion of the contract then the contractor will either return all data to the Authority or provide a certificate of secure destruction using an industry and Authority approved method. Destruction or return of the data will be decided by the Authority at the time of termination of the services provided under the contract.

Appendix 1- Outline Security Plan

For and on Behalf of the Supplier – 7 SAFE LIMITED:

Name and Title	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted] on Behalf of the Customer – CARE QUALITY COMMISSION

Name and Title	[redacted]
Signature	[redacted]
Date	[redacted]