secarma®
CYBERSECURITY EXPERTS

Penetration Testing and Assurance Services

Standard Terms and Conditions

Prepared for G-Cloud 14 (RM1557.14)

Author: Alex Methley
Date: 06/05/2024
Version: 2.0

Contents

Contents 1
1. INTRODUCTION 2
1.1.1 Description 2
2. DEFINITIONS 2
3. COMPANY'S DUTIES 4
4. THE CLIENT AGREES 5
5. FEES AND PAYMENT 7
6. CONFIDENTIALITY 8
7. INTELLECTUAL PROPERTY RIGHTS 8
8. LIABILITY 9
9. TERMINATION 10
10. EXCLUSION OF THIRD PARTY RIGHTS 10
11. DATA PROTECTION 10
12. FORCE MAJEURE 12
13. GENERAL 12

1. INTRODUCTION

1.1.1 Description

Secarma Limited provide specialist Penetration Testing, Security Assurance and Security consultancy services through the Government Procurement Service (GPS) G-Cloud catalogue. The services provided, as currently listed in the G-Cloud Digital Marketplace are the following:

- Penetration Testing Services
- Vulnerability Assessment Services
- Cyber Essentials Certification
- Cyber Essentials Plus Certification
- IoT Cyber Baseline and Cyber Assurance Level 1 & 2 Certification Services
- IT Health Check Assessment Services
- Social Engineering and Adversary Simulation Services
- Objective Led Testing and Red/Purple Team Services
- Cloud Security Configuration Review Services
- Incident Response Scenario Wargaming Services
- Cyber Security Maturity Assessment Services
- Threat Modelling Services

The Terms & Conditions applicable to services listed in the GPS G-Cloud Digital Marketplace, which may be engaged by a G-Cloud customer who wishes to proceed with Secarma Limited as a supplier are detailed in this document.

2. DEFINITIONS

2.1. “Penetration Test Authorisation Form” means the Company’s form to be signed by the Client and submitted to Company when ordering the Security Testing;

2.2. “Client” means the individual(s) and/or organisation(s) to whom the Company is providing Security Testing and who has signed and completed a Penetration Test Authorisation Form;

2.3. “Company” means Secarma Limited (Company Registration Number: 04217114)

2.4. “Conditions” means the terms and conditions set out in this Contract;

2.5. “Confidential Information” means all tangible and intangible information designated as confidential by any party in writing together with all other information which may reasonably be regarded as confidential including, but not limited to, details of the Clients’ System, procedures, network configuration and topology, passwords, private encryption keys and details of the Company’s methodologies;

2.6. “Consultant” means the individual(s) provided by Company for the performance of the Security Testing;

2.7. “Contract” means the contract formed by these Terms and Conditions together with the Proposal and the Penetration Test Authorisation Form;

2.8. “Data Protection Laws” shall mean: (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data; and (ii) on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

2.9. “Event of insolvency” means if the Client is unable to pay its debts (within the meaning of Section 123 of the Insolvency Act 1986) or becomes insolvent, or is subject to an order or a resolution for its liquidation, administration, winding-up or dissolution (otherwise than for the purposes of a solvent amalgamation or reconstruction), ceases or threatens to cease to carry on its business or has an administrative or other receiver, manager, trustee, liquidator, administrator or similar officer appointed overall or any substantial part of its assets, or enters into or proposes any composition or arrangement with its creditors generally, or is subject to any analogous event or proceeding in any applicable jurisdiction;

2.10. “Fees” means Company’s fees for the Security Testing as detailed in the Proposal, and all reasonable expenses incurred by the Consultant in carrying out the Security Testing which will be agreed in advance with the Client;

2.11. “Force Majeure” means any cause preventing either Party from performing any or all of its obligations under these Conditions which arises from or is attributable to acts, events, omissions or accidents beyond the reasonable control of the Party so prevented;

2.12. “Intellectual Property Rights” (IPR) means any copyright, patent, design patent, registered design and design rights, utility models, trademarks, service marks, an application for any of these or the right to supply for the same, trade secrets, know-how, database rights, moral rights, confidential information, trade or business names and any other industrial and proprietary and other similar protected rights in any country and any licences under or in respect of such rights;

2.13. “Party” means any party to, or the parties to, this Contract;

2.14. “Personal Data” has the meaning given to that term in Data Protection Laws;

2.15. “Proposal” means the proposal for the Security Testing provided by Company to the Client detailing the scope of work all or some of which may be accepted by the Client in their purchase order;

2.16. “Security Testing” means the provision of services as described in the Proposal made by the Company to the Client;

2.17. “Start Date” means the date the Security Testing will start to be provided as confirmed by the Company in writing to the Client;

2.18. “System” means the systems, networks, processes and policies, whether technical or not, which the Client requires to be security tested described in the Proposal made by the Company to the Client and pursuant to this Contract;

2.19. “Test Report” means the report produced by the Company detailing the results of the Security Testing;

2.20. “VAT” means value added tax as defined under the Value Added Tax Act 1994.

3. COMPANY’S DUTIES

3.1. The Company shall perform the Security Testing for the Client using reasonable skill and care and in a professional, timely manner. Time for

provision or completion of the Security Testing or any part of it shall not be of the essence.

3.2. Where a Test Report is required it shall, unless otherwise agreed, be produced by the Consultant within ten (10) working days or as agreed with the Client on completion of the Security Testing and sent to the Client.

3.3. Whilst the Company will use reasonable endeavours to ensure that the same Consultant will continue throughout the Security Testing, it reserves the right to replace that Consultant if necessary at its reasonable discretion by notifying the Client.

3.4. The Company shall, where the Consultant is present on the Client's premises, ensure that the Consultant complies with such reasonable site rules and procedures as are prior notified to the Company.

4. THE CLIENT AGREES

4.1. To obtain appropriate consent from its ISP (Internet Service Provider), only where the ISP is hosting services on behalf of the Client and any other relevant third party supplier of the System, only where the third party supplier is hosting services on behalf of the Client for the Security Testing to be carried out and, when requested by the Company, to provide evidence of such consent and to notify relevant employees that the Security Testing has been scheduled and that they may be monitored;

4.2. To arrange a mutually convenient time with the Company for the performance of the Security Testing and to inform its ISP of the date agreed with Company in accordance 4.1;

4.3. To make appropriate backups of the System prior to the commencement of the Security Testing;

4.4. That, where the Security Testing is to take place on the Client's premises, the Client shall ensure that suitable accommodation is provided for the Consultant which shall include network access and, where necessary, access to data centres, server rooms and/or switch rooms;

4.5. That should the Client require a laptop or Personal Digital Assistant (PDA) to be security tested by the Company it will deliver the laptop

and/or PDA to the Company's registered address and collect it from those premises or authorise other means of delivery and return at the Client's own risk. The Company shall not be liable for the laptop or PDA during transit to or from its offices;

4.6. The Client will compensate the Company for any direct losses incurred as a result of a claim from a third party arising out of any failure of the Client to comply with clauses 4.1, 4.2 and 4.3 provided always that the Company shall mitigate any and all losses and provide written notice of any claim to the Client within 10 working days;

4.7. To provide the Company with at least one employee who shall have substantial computer systems, network and project management experience of the Client's Systems to act as liaison between the Client and the Company;

4.8. To co-operate with the Company and to provide it promptly with such information about its Systems, network, premises, equipment, data structures, protocols, software, hardware and firmware as are reasonably required by the Company;

4.9. To ensure that, where the Security Testing is taking place on its premises, the premises are safe;

4.10. That, by signing the Penetration Test Authorisation Form, the Client consents, for itself and on behalf of all group companies, to the Company performing the Security Testing and that it has procured, where necessary, the consent of all its (and its group companies) employees, agents and sub-contractors that the Company shall be permitted to carry out the Security Testing. The Company will be carrying out the Security Testing in the belief that it has all appropriate consents, permits and permissions from the Client and its group companies (and their employees, agent and sub-contractors);

4.11. That, whilst the Company will conduct all Security Testing in line with accepted best practice and make all reasonable efforts to avoid disruption of the Client's network, the tools and techniques used may cause disruption to the Client's Systems and/or possible loss of or corruption to data and the Client agrees to take such backups and provide such redundant systems as are prudent in the circumstances. The Company will notify the Client in the event where activity would lead to loss of service or data before proceeding where this is known to the Company;

4.12. To notify the Company immediately if there are any periods during Security Testing when the Company should stop work due to critical business processes (such as batch runs) or if any part of the System is business critical so that the Company can, if needs be and with the Client's consent, modify its testing approach;

4.13. That, where the Company supplies any software as part of the Security Testing, it shall only use such software for lawful purposes;

4.14. That, during the performance of the Security Testing and for a period of 6 months after completion of the Security Testing, it will not recruit any employees or personnel of the Company which it met or was introduced to through its relationship under this Contract without the prior written consent of the Company;

5. FEES AND PAYMENT

5.1. Subject to 5.2 below and unless otherwise agreed, the Fees payable under this Contract shall be invoiced on delivery of the Test Report or, if none is to be provided, on completion of the Security Testing. Invoices are due for payment within 30 days of the date of the invoice. All payments due under this Contract shall become due immediately upon termination of this Contract despite any other provision in this Contract. All payments due under this Contract shall be made without any deduction by way of set off, counterclaim, discount or abatement or otherwise.

5.2. The Company shall be entitled to interest on any payment not paid when properly due pursuant to the terms of these conditions, calculated from day to day at a rate per annum equal to 3% above the base rate of National Westminster Bank Plc and payable from the day after the date on which payment was due up to and including the date of payment (whether before or after judgment).

5.3. All sums under the Contract are unless otherwise stated, exclusive of VAT. Any VAT payable in respect of such sums shall be payable in addition to such sums and shall be payable in addition to such sums, at the rate from time to time prescribed by law on delivery of a valid VAT invoice.

5.4. The Company reserves the right to invoice the Client upon acceptance of the order an amount of 10% of the estimated Fees that will be charged for the performance for the Security Testing to cover

the costs of initiating and preparing for the performance of the Security Testing ("Initial Fee"). The Initial Fee will be treated as a payment on account of the total Fees charged for the Security Testing.

5.5. Upon confirmation by the Company in writing to the Client of the Start Date, the Company will immediately start to allocate resources and facilities and commit to third party expenditure to fulfil its contractual commitments. The Company may at its absolute discretion allow the Security Testing to be re-scheduled or cancelled, but if it does so allow, the Client agrees that it will be committed to paying the Company a proportion of the Fees as genuinely pre-estimated liquidated damages to reflect the losses which it will incur as a result of such cancellation or re-scheduling, as follows:

5.5.1. cancellation or re-schedule request within 120 hours of the start date and where the Company is unable to utilise the committed resources up to 100% of the Fees will be payable; and

5.5.2. this applies to each delay separately. Where the Company permits a re-booking, in addition to the proportion of the Fees incurred above, the full Fees will also be payable for the Security Testing as re-booked.

6. CONFIDENTIALITY

6.1. Each party will not disclose or permit its employees, agents and sub-contractors to disclose any Confidential Information entrusted to it by the other party provided always that this restriction shall not apply to information already in the receiving party's possession, or which comes into the public domain other than by breach of this obligation by the receiving party or its employees, agents and sub-contractors, or which is disclosed to the receiving party or which is required to be disclosed pursuant to any law or regulation or by the rules of any stock exchange or by a court of competent jurisdiction. If Confidential Information is required to be disclosed pursuant to any law or regulation or by the rules of any stock exchange or by a court of competent jurisdiction then the Receiving Party shall notify the Disclosing Party prior to any disclosure.

7. INTELLECTUAL PROPERTY RIGHTS

7.1. Ownership of all Intellectual Property Rights in the System remains at all times with the Client and/or its ISP or other third party supplier. For

the avoidance of doubt, all Intellectual Property Rights in the materials used by the Company to carry out the Security Testing remain vested in the Company or any relevant third party owners.

7.2. All Intellectual Property Rights in the results of the testing shall belong to the Client.

7.3. Copyright in the Test Report shall also remain with the Company, but the Client is hereby granted a non-exclusive, non-transferable licence to copy and use the Test Report for its own internal purposes only. The Client will need prior agreement to be sent in any form to any 3rd party. In any event this will not be given to the forwarding of a Test Report to a penetration testing company or entity.

8. LIABILITY

8.1. Nothing in this clause 8 excludes or limits the liability of the Company for fraudulent misrepresentation or for death or personal injury caused by the Company's negligence. Save as aforesaid the following provisions set out the entire financial liability of the Company (including any liability for the acts or omissions of its employees, agents and sub-contractors) to the Client, its ISP or any third party supplier of the System to the Client.

8.2. The Company shall not be liable for any loss, damage, costs, expenses or other claims for compensation arising from any material or instruction supplied by the Client which are incomplete, incorrect, inaccurate, illegible or defective in any other way. The Company should highlight to the Client any known errors.

8.3. The Company shall not be liable for any loss or damage caused to either the Client, its ISP or other third party supplier of the System either jointly or severally except to the extent that such loss or damage is caused by the negligent acts or omissions of or a breach of any contractual duty by the Company, its employees, agents or sub-contractors in performing the Security Testing.

8.4. The Company's total liability in respect of all claims arising under or by virtue of this Contract or in connection with the performance of this Contract shall not exceed £1,000,000 in aggregate.

8.5. The Client's total liability in respect of all claims arising under or by virtue of this Contract or in connection with the performance of this Contract shall not exceed the amount £1,000,000 in aggregate.

8.6. The Company and the Client shall not be liable to each other for any indirect or consequential loss or damage whether for loss of profit, loss of business, depletion of goodwill or otherwise whatsoever or howsoever caused which arise out of or in connection with this Contract even if such loss was reasonably foreseeable

9. TERMINATION

9.1. The Company reserves the right to withdraw or delay from Security Testing by providing 5 working days' notice, if, in its opinion, information required for satisfactory completion of the Security Testing and requested by the Company in writing is either not provided or, if provided, is inaccurate or inadequate. The Client shall be liable for any reasonable fee and expenses incurred up to and including the date of withdrawal.

9.2. Either party may (without limiting any other remedy) at any time terminate the Contract by giving written notice to the other if the other commits any material breach of these Conditions and (if capable of remedy) fails to remedy the breach within thirty (30) days after being required by written notice from the other Party to do so, or in an Event of Insolvency.

10. EXCLUSION OF THIRD PARTY RIGHTS

A person who is not a party to this Contract shall not have any rights under the Contract (Rights of Third Parties) Act 1999 to enforce any term of this Contract

11. DATA PROTECTION

11.1. In the course of providing the Security Testing, the Company may obtain Personal Data from the Client. The Client confirms that it has obtained all consents required from data subjects to enable such Personal Data to be disclosed to the Company and made all necessary

registrations and notifications in accordance with applicable Data Protection Laws to enable the Company to carry out the Security Testing and the Client will ensure the same are kept accurate and up to date.

11.2. In respect of any Personal Data held or processed by the Company as a result of or pursuant to these Conditions, the Company represents to the Client that it has made all necessary registrations and notifications in accordance with applicable Data Protection Laws and that it will ensure that the same are kept accurate and up to date during the term of the agreement.

11.3. In addition to and notwithstanding any other right or obligation arising under these Conditions, the Company (and shall ensure that its Personnel shall):

a) implement appropriate technical and organisational measures to protect the Personal Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to the Data (a "Security Incident").
b) use the Personal Data obtained as a result of these Conditions only for the purposes of fulfilling its obligations under these Conditions and not disclose Personal Data without the written authority of the Client;
c) comply with the express instructions or directions of the Client from time to time in connection with the use of such Personal Data and the requirements of any Data Protection Laws and such Personal Data shall be treated as Confidential Information of the Client for the purposes of these Conditions;
d) not do or omit to do anything which causes the Client to breach any Data Protection Laws or contravene the terms of any registration, notification or authorisation under any Data Protection Laws of the Client; and
e) not transfer Personal Data which has been obtained by or made available to the Company to any country outside the European Economic Area without the prior written consent of the Client.
11.4. The Company shall not subcontract any processing of the Personal Data to a third party subcontractor without the prior written consent of the Client. If the Client refuses to consent to the Company's appointment of a third party subcontractor on reasonable grounds relating to the protection of the Personal Data, then the Company will not appoint the subcontractor.

11.5. The Company shall not be in breach of this Clause 11 if it acts on the instructions of the Client.

11.6. If the Company believes or becomes aware that its processing of the Personal Data is likely to result in a high risk to the data protection rights and freedoms of data subjects, it shall inform the Client as soon as reasonably practicable and provide the Client with all such reasonable assistance at the Client's cost as the Client may reasonably require in order to conduct a data protection impact assessment.

11.7. The Company will (and will ensure that its Personnel will) without undue delay notify the Client if it becomes aware of a Security Incident or if lawfully able that a disclosure of Personal Data may be required by law, or if it receives a request from an individual to access their Personal Data or to cease or not begin processing (or to rectify, block, erase or destroy Personal Data), or if it receives any communication from the Office of the Information Commissioner or similar authority relating to the Personal Data. The Company shall provide all such timely information and cooperation as the Client may reasonably require in order for the Client to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Data Protection Laws. The Company shall further take all such measures and actions as are technically practicable and within its control to remedy or mitigate the effects of the Security Incident and shall keep the Client up-to-date about all developments in connection with the Security Incident.

12. FORCE MAJEURE

12.1. Neither party to the Contract shall be deemed to be in breach of these conditions or otherwise liable to the other party in any manner whatsoever for any failure or delay in performing its obligations to the extent that the same is caused by Force Majeure. In the event the Force Majeure continues for a continuous period in excess of thirty (30) working days, either party shall be entitled to give notice in writing to the other party.

13. GENERAL

13.1. The Consultant shall have no authority to amend the terms and conditions of this Contract or to relieve the Client of any of its obligations under these conditions or to increase the Company's obligations under these conditions or waive any of the Company's rights under these terms and conditions. The Consultant shall have no authority to incur expenditure in the name of or an account of the

Company or hold themselves out as having authority to bind the Company.

13.2. The Company does not give any warranty or undertaking or make any representation (either express or implied) as to the completeness or accuracy of any information provided to the Client prior to this Contract which relates to or is provided in respect of these terms and conditions by or on behalf of the Company.

13.3. These standard terms and conditions together with the Penetration Test Authorisation Form and the Proposal, shall constitute the entire agreement between the Parties and supersede any previous agreement or understanding and may not be varied except in writing between the Parties and signed by their respective authorised signatories. All other terms and conditions express or implied by statute or otherwise, are excluded to the fullest extent permitted by law. As regards Security Testing, in the event of any conflict between any of the terms of these documents the following order shall prevail:

(1) Penetration Test Authorisation Form;

(2) the terms and conditions in this Contract; and

(3) Proposal.

13.4. Any notice sent under this Contract shall be in writing addressed to the other Party at its registered office or principal place of business or such other address as may be notified by each Party to the other time to time.

13.5. No failure or delay by either party in exercising any of its rights under this Contract shall be deemed to be a waiver of that right.

13.6. If any provision or any part of a provision of this Contract is held by any authority to be invalid and unenforceable, the validity of the other provisions and/or the remaining part of the provision shall not be affected.

13.7. This Contract shall be governed by the laws of England and the Parties submit to the exclusive jurisdiction of the English courts, except for enforcement proceedings where the English courts shall have non-exclusive jurisdiction.

If you have any further questions regarding Secarma's terms and conditions. Please contact us at enquiries@secarma.com