

Terms of service for security testing and consultancy

11th July 2019

1. Parties

- 1.1. This agreement is between Dxw Cyber Ltd, a company registered in England and Wales under number 10984430 and with registered address 8-9 Hoxton Square, London, United Kingdom, N1 6NU, trading as “dxw cyber” (“our”, “we”) and the organisation or person specified on the order summary (the “Order Summary”) accompanying this document (“you”, “your”).

2. Definitions

2.1. Adverse Impact

An Adverse Impact is any downtime, degradation or loss of service, destruction or corruption of data, loss of confidentiality or other impairment of computer hardware, software or data that occurs as a direct or indirect consequence of security testing.

2.2. Fees

The fees payable by you for the Work, as set out in the Order Summary.

2.3. Goals

The Goals are the purpose for and desired results of the Work, as stated in the Order Summary.

2.4. Host

A Host is computer or other electronic device able to process information.

2.5. Team

The Team is the dxw cyber employees (and/or other freelancers or contractors) that undertake the Work.

2.6. Personal Data

Personal Data is any information relating to a directly or indirectly identifiable natural person.

2.7. Required Materials

Required Materials are materials that dxw cyber reasonably needs in order to complete the Work, including but not limited to source code, access credentials for Hosts or services, documentation, answers to written questions, or any other materials reasonably requested.

2.8. **Work**

The services provided by the Team under this agreement with the aim of achieving the Goals, as set out in the Order Summary.

3. **The Work**

- 3.1. dxw cyber will provide the Team for the period of time specified in the Order Summary to undertake the Work in return for payment by you of the Fees.
- 3.2. The Goals represent our best understanding of the purpose for and desired results of the Work, at the date of the Order Summary.
- 3.3. If, at any time during the Work, the Goals you wish to address change materially, you must notify us, and new Goals must be agreed in writing.
- 3.4. If the Goals are changed during the work, dxw cyber reserve the right to provide a new Order Summary, with different Fees payable for the Work. Our agreement to the updated Goals will be contingent on your acceptance of any associated change in Fees.
- 3.5. dxw cyber may review and revise the Fees associated with the Order Summary annually on the anniversary of the commencement date. Where this happens, dxw cyber will send you an updated Order Summary.
- 3.6. The Order Summary is not a specification nor a commitment to produce specific deliverables; it is a commitment to provide the Team for the amount of time defined in the Order Summary.
- 3.7. dxw cyber does not guarantee that the Goals of the Work will be achieved.

4. **General enquiries**

- 4.1. Where the duration of the Work is more than one month and involves the payment of a regular monthly fee, you may contact us as necessary with enquiries or questions of a general security nature.
- 4.2. As far as is practical, we will give advice or comments that we hope may be of assistance at no additional cost.
- 4.3. This provision does not apply where the giving of advice or comments to a professional standard requires background research, analysis, discussion or specialist guidance.
- 4.4. Our ability and capacity to be able to respond to general enquiries will vary depending on our workload. We are not able to guarantee any particular speed of response or level of service.

5. **Scope of work**

- 5.1. Prior to the commencement of any practical security testing that may form part of the Work, the parties must agree in writing to a scope for the testing (the “Scope”).
- 5.2. The Scope will list the hosts (the “Hosts”) against which dxw cyber is authorised to perform practical security testing as part of the Work.
- 5.3. During the Work, either party may request amendments to the Scope.
- 5.4. Changes to the Scope will not affect the amount of time the Team spend on the Work nor the fees due for the Work. However, both parties acknowledge that prompt agreement to changes to the Scope is necessary for the Goals to be met and that unnecessary narrowing of the scope or placing other restrictions on the practical security testing increase the risk that the Goals will not be achieved.

6. **Consent to practical security testing**

- 6.1. dxw cyber may, where the acts are lawful without your consent or where the acts are sufficiently routine in nature that consent can be implied, carry out practical security testing, research and analysis relating to information or programs from, on or about any of your Hosts. Such acts might include (but are not limited to) examining publicly available open source intelligence regarding the Hosts, such as DNS records and SSL certificates or making routine SMTP, HTTP or HTTPS requests to the Hosts.
- 6.2. dxw cyber will not perform any practical security testing that would otherwise be unlawful without your consent in the form of the Scope.
- 6.3. In respect of the Hosts set out in the Scope, you authorise dxw cyber to:
 - 6.3.1. Access or modify programs and data on the Hosts, which may include Personal Data;
 - 6.3.2. Perform actions on the Hosts which may impair their operation, prevent or hinder access by other users, or impair the operation of programs that run on them;
 - 6.3.3. Intercept or modify communications to and from the Hosts or between any other Hosts on a network to which any of the Hosts are connected;
 - 6.3.4. Make false or misleading representations to your employees as part of the Work, and you acknowledge and agree that the intent of these statements is not malicious but instead is to make assessments of your security;
- 6.4. At the conclusion of testing, dxw cyber will, as far as is reasonably practical, ensure each Host subjected to testing is restored to a state substantially similar to that in which it was found at the start of testing.

7. Data protection

7.1. In this clause:

- 7.1.1. Data Protection Legislation means the UK Data Protection Legislation and (for so long as and to the extent that the law of the European Union has legal effect in the UK) the General Data Protection Regulation ((EU) 2016/679) and any other directly applicable European Union regulation relating to privacy.
- 7.1.2. UK Data Protection Legislation means any data protection legislation from time to time in force in the UK including the Data Protection Act 1998 or 2018 or any successor legislation.
- 7.1.3. In this section, Host Personal Data means Personal Data that we access from your Hosts or that is given to us by you to support or enable practical security testing.
- 7.1.4. Other Personal Data that we collect are processed in order to perform our obligations under this agreement, in accordance with our Privacy Policy as published on our website and amended from time to time.

7.2. You recognise and agree that the nature of practical security testing makes it impractical to explicitly state what categories of personal data may be processed in advance of that data being found during testing. As part of undertaking the Work, dxw cyber may:

- 7.2.1. incidentally access Host Personal Data that is present on one or more of the Hosts;
- 7.2.2. need to include limited amounts of Host Personal Data in its reports to you as part of describing any vulnerabilities or other findings which were identified during the Work;
- 7.2.3. need to undertake processing off-site of some categories of Host Personal Data for the purpose of working towards the Goals, for example:
 - 7.2.3.1. analysis of usernames and passwords, whether hashed, encrypted or in plaintext;
 - 7.2.3.2. finding identifiers that may be used to locate a given user in other systems, for example, social media usernames, IP addresses or alternative email addresses;
 - 7.2.3.3. analysis of the contents of text fields, including where structured or obfuscated, for example profile descriptions or private messages.

7.3. dxw cyber shall delete any Host Personal Data under sub-clause 2 above within 90 days of termination of this agreement, save that dxw cyber shall be permitted to:

- 7.3.1. retain hashed or encrypted passwords and their plaintext equivalents (but not associated usernames) indefinitely for the purpose of security research, the same not constituting Personal Data under Data Protection Legislation;
- 7.3.2. retain copies of our notes and of any reports prepared for you as part of the Work, which may incidentally contain Host Personal Data or other Personal Data.

7.4. In respect of Personal Data:

- 7.4.1. Both parties will comply with all applicable requirements of the Data Protection Legislation.

- 7.4.2. The parties acknowledge that for the purposes of the Data Protection Legislation, you are the data controller and dxw cyber is the data processor (where Data Controller and Data Processor have the meanings as defined in the Data Protection Legislation) in respect of the Host Personal Data.
- 7.4.3. Without prejudice to the generality of sub-clause 1 above, you will ensure that you have all necessary lawful bases, consents and notices in place to enable lawful transfer of the Host Personal Data to dxw cyber for the duration and purposes of this agreement.
- 7.4.4. Without prejudice to the generality of sub-clause 1 above, dxw cyber shall, in relation to any Host Personal Data processed in connection with this agreement:
- 7.4.4.1. process that Host Personal Data only in accordance with these terms or on your written instructions unless we are required by applicable laws otherwise to process that Host Personal Data;
 - 7.4.4.2. ensure that we have in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Host Personal Data and against accidental loss or destruction of, or damage to, Host Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures;
 - 7.4.4.3. ensure that all personnel who have access to and/or process Host Personal Data are obliged to keep the Host Personal Data confidential;
 - 7.4.4.4. not transfer any Host Personal Data outside of the European Economic Area;
 - 7.4.4.5. assist you, at your cost, in responding to any request from a Data Subject and in ensuring compliance with your obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;
 - 7.4.4.6. notify you without undue delay on becoming aware of a Host Personal Data breach;
 - 7.4.4.7. at your written direction, delete or return Host Personal Data and copies thereof to you on termination of the agreement unless required by applicable law to store the Host Personal Data; and
 - 7.4.4.8. maintain complete and accurate records and information to demonstrate its compliance with this clause.

8. Required Materials

- 8.1. Where reasonably required by the Team for the Work, the Team may request Required Materials that you must provide.

- 8.2. You must provide Required Materials as soon as is reasonably practical. If you are unable or unwilling to provide such Required Materials, you acknowledge that it may not be possible to complete all or part of the Work, nor to achieve the Goals, but this will not affect the fees due under this agreement which will still be payable by you.

9. Engagement

- 9.1. It is essential that you fully engage with the Work in order for the Goals to be met. You must promptly:
 - 9.1.1. Participate actively in the Work as reasonably required;
 - 9.1.2. Respond to our enquiries in a reasonable timeframe;
 - 9.1.3. Supply to us any Required Materials;
 - 9.1.4. Report any issue or problem that could affect the Work;
 - 9.1.5. Report any issue or problem that may be an Adverse Impact or could potentially give rise to an Adverse Impact.

10. Subcontracting

- 10.1. In dxw cyber's absolute discretion, freelancers or contractors may be used in place of dxw cyber employees to undertake any part of the Work.
- 10.2. dxw cyber will not outsource (ie, allow to be completed without our direct supervision) any part of the Work without your prior agreement, which must not be unreasonably withheld or delayed.

11. Quality

- 11.1. dxw cyber will complete the Work with reasonable skill, care and diligence, in accordance with good industry practice.
- 11.2. dxw cyber will take steps to ensure, as far as is reasonably practical, that:
 - 11.2.1. Its advice, findings and recommendations are accurate and applicable;
 - 11.2.2. Its work does not cause Adverse Impacts.
- 11.3. Due to the nature of the Work, dxw cyber cannot guarantee that its advice, findings and recommendations will be complete or accurate in every detail, nor that all vulnerabilities present on the Hosts will be identified.

12. Limitation of liability

- 12.1. dxw cyber will maintain an appropriate level of insurance against professional negligence at all times.

- 12.2. You acknowledge that all security work of a practical nature carries the risk of Adverse Impacts, and that it is not reasonably practical or possible for those risks to be eliminated or made inconsequential. You accept the risk of Adverse Impacts when the Work is being undertaken.
- 12.3. You agree that it is your responsibility to ensure that you put in place measures that ensure a level of resilience in the Hosts to preserve your ability to continue to operate in the event of an Adverse Impact. dxw cyber can work with you to design or implement such measures at your request.
- 12.4. Subject to sub-clause 5 below, the following types of loss are wholly excluded by the parties:
 - 12.4.1. Loss of profits.
 - 12.4.2. Loss of sales or business
 - 12.4.3. Loss of agreements or contracts.
 - 12.4.4. Loss of anticipated savings.
 - 12.4.5. Loss of use or corruption of software, data or information or other Adverse Impacts.
 - 12.4.6. Loss of or damage to goodwill or reputation.
 - 12.4.7. Indirect or consequential loss.
- 12.5. Nothing in this agreement should be read as excluding our liability for death or personal injury caused by our negligence, fraud or fraudulent misrepresentation or any other liability that cannot legally be limited.
- 12.6. In any event, either party's total liability (which term includes liability in contract, tort (including negligence), breach of statutory duty, or otherwise, arising under or in connection with the agreement) is limited to three times the total fees paid for the Work in the twelve months prior to the incident giving rise to the alleged liability taking place.
- 12.7. You shall indemnify dxw cyber against all liabilities, costs, expenses, damages and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other professional costs and expenses) suffered or incurred by dxw cyber arising out of or in connection with any testing dxw cyber performs against a Host you authorise to include in the Scope without lawful authority.

13. Confidentiality

- 13.1. Subject to subclauses (2) and (3), dxw cyber will keep your status as a client and all details of the Work strictly confidential.
- 13.2. dxw cyber will not keep confidential any information which:
 - 13.2.1. Pertains to the tools, techniques, approaches and methodologies we use in our work in general;

- 13.2.2. Is in the public domain (other than through our default) or which we receive from a third party who is lawfully entitled to disclose it;
 - 13.2.3. Is known by us prior to receipt of the information from you;
 - 13.2.4. Is developed by us independently of information obtained as part of our relationship with you;
 - 13.2.5. It is required by law to disclose.
- 13.3. In respect of security vulnerabilities we discover in third party software or systems during the Work, we may, without identifying you:
 - 13.3.1. Publish details of the vulnerability in accordance with our Responsible Disclosure Policy, as published on our website and varied from time to time;
 - 13.3.2. Provide details of the vulnerability to any other person;
 - 13.3.3. Disclose details of the vulnerability to national authorities.
- 13.4. You must limit the sharing of any document or report we supply to you as part of the work to that necessary in order to achieve the Goals.
- 13.5. Where it is necessary to share a document with a party outside your organisation in order to achieve the Goals, you must place that party under conditions of confidentiality equivalent to or stronger than these terms.
- 13.6. You may not disclose information about a security vulnerability discovered by dxw cyber in third party software to any person, including its vendor, unless:
 - 13.6.1. You have dxw cyber's written agreement to the disclosure; or
 - 13.6.2. More than four weeks have passed since the discovery of the vulnerability by dxw cyber.
- 13.7. In the event that, in accordance with these terms, you disclose information about a security vulnerability to any person, you must place them under conditions of confidentiality equivalent to or stronger than these terms which shall remain in effect until software or instructions resolving the security vulnerability are released and available to users of the software.
- 13.8. In the event that you, or a party you have disclosed information to, publish information about a security vulnerability discovered by dxw cyber, you must ensure that dxw cyber is clearly and prominently credited for its discovery, and that a link to www.dxwcyber.com is included in the published information.

14. Intellectual property

- 14.1. All intellectual property created by dxw cyber or any member of the Team in the course of the Work remains owned by us.

- 14.2. All intellectual property created by you in the course of the Work, or that you have created prior to the Work commencing, remains owned by you.
- 14.3. Where dxw cyber provides you with a deliverable that contains our intellectual property, we grant you a perpetual, irrevocable, non-exclusive, royalty-free licence to use that intellectual property, solely for the purpose of achieving the Goals.
- 14.4. You must not use nor distribute materials containing dxw cyber's intellectual property for any purpose (whether commercial or otherwise) other than achieving the Goals, without our prior written consent.
- 14.5. You grant dxw cyber a non-exclusive, royalty-free licence to use your intellectual property where necessary in order to achieve the Goals, and strictly for no other purpose.

15. Payments

- 15.1. dxw cyber will issue invoices for the Fees as set out in the Order Summary.
- 15.2. dxw cyber requires payment of a fifty percent deposit for any one-off fees that form part of the Order Summary before delivery dates for work can be confirmed. The remaining fifty per cent of the Fees shall be paid upon completion of the Work as set out in the Order Summary.
- 15.3. dxw cyber's invoices must be paid within 30 days.
- 15.4. dxw cyber may charge interest on overdue amounts at 8% over the Barclay's Bank base rate.
- 15.5. You shall make payment by BACS or CHAPS transfer. dxw cyber does not accept cheques.
- 15.6. You are responsible for any fees associated with making a payment to dxw cyber.
- 15.7. VAT (where applicable) is payable on, and in addition to, all sums due under this agreement.
- 15.8. dxw cyber issues invoices by email. If you require a paper invoice to be issued, dxw cyber may charge an additional fee.

16. Termination

- 16.1. Either party may terminate this agreement at any time by giving 60 days' notice in writing.
- 16.2. dxw cyber may terminate this agreement with immediate effect by giving written notice to you if you fail to pay any amount due under this agreement on the due date for payment and remains in default not less than 14 days after being notified in writing to make such payment;

- 16.3. Without affecting any other right or remedy available to it, either party may terminate this agreement with immediate effect by giving written notice to the other party if:
- 16.3.1. the other party repeatedly breaches any of the terms of this 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 of this agreement;
 - 16.3.2. the other party's staff engage in a course of conduct which is threatening, abusive, amounts to harassment or otherwise threatens the wellbeing of the terminating party's staff;
 - 16.3.3. the other party suspends, or threatens to suspend, payment of its debts or is unable to pay its debts as they fall due, admits inability to pay its debts, or enters into an arrangement with creditors;
 - 16.3.4. a petition is filed to wind up the other party or an administrator is appointed.
- 16.4. If dxw cyber terminates this agreement, we will provide you with a summary of your account with us. We will refund any fees paid for work we have not yet delivered, and you will pay any fees due for Work delivered but not yet paid.
- 16.5. If you terminate this agreement, you forfeit any fees we have invoiced for work agreed but not yet delivered, including any deposit you have paid.
- 16.6. Where the Order Summary states that the Work has an end date, the agreement will terminate 90 days after the Work has been completed unless it is extended, in which case dxw cyber will provide a new Order Summary.
- 16.7. The parties' obligations under sections 7.3, 12, 13, 14 and 15 will survive termination of this agreement.

17. Circumstances beyond the parties' control

- 17.1. Neither party shall be in breach of this agreement nor liable for delay in performing, or failure to perform, any of its obligations under this agreement if such delay or failure result from events, circumstances or causes beyond its reasonable control.
- 17.2. In such circumstances the affected party shall be entitled to a reasonable extension of the time for performing such obligations.

18. Changes to these terms

- 18.1. Changes to these terms may be made in writing by mutual agreement of the parties, which must not be unreasonably withheld.

19. Notices

- 19.1. Any notice or other communication given to a party under or in connection with this agreement shall be in writing and shall be sent by email to the address specified in the Order Summary
- 19.2. Any notice or communication shall be deemed to have been received at the time of transmission, or, if this time falls outside business hours in the place of receipt, when business hours resume.
- 19.3. This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

20. Headings

- 20.1. The section headings contained in this agreement are for reference only and shall not in any way affect the meaning or interpretation of this agreement.

21. Miscellaneous

- 21.1. With the exception of any framework agreement of which this agreement forms a part, this agreement and the Order Summary that accompanies it constitute the entire agreement between us with respect to the Work, and replaces any prior oral or written agreement which may exist.
- 21.2. If any provision of this agreement is found by any court, tribunal or administrative body of competent jurisdiction to be wholly or partly illegal, invalid, void, voidable, unenforceable or unreasonable it shall to that extent be deemed severable and the remaining provisions of the agreement and the remainder of such provision shall continue in full force and effect.
- 21.3. The parties to this agreement do not intend that any term of this agreement will be enforceable by virtue of the Contracts (Rights of Third parties) Act 1999 by any person that is not a party to it.

22. Jurisdiction and choice of law

- 22.1. This agreement is governed by English law and the parties agree that any disputes arising from the agreement will be subject to the exclusive jurisdiction of the courts of England and Wales.