

Terms & Conditions:

These terms and conditions together with our Privacy Notice and our Acceptable Use Policy (together, the 'Terms') provide you with information about us and apply to any contract between you and us. Please read these Terms carefully and make sure you understand them before ordering anything from our website. We will also notify you, at the point of purchase if there are any additional terms and conditions that may apply to any specific contract made between us.

Our prices are as set out on our website, do not include packaging, shipping, insurance, or travel costs, and are subject to the addition of applicable VAT or other state or national tax in line with any relevant regulations.

We may vary our prices from time to time, which we will do by updating our website. Price changes will not be retrospective.

CYBER ESSENTIALS AND CYBER ESSENTIALS PLUS:

We will upon receipt of the Fees give you access to the self-assessment portal within 24 hours of the order being processed and will, under this agreement, assess the completed questions.

If consultation has been purchased, we will send through a secure email within 24 hours to the contact provided at the time of purchasing to arrange a Teams meeting for the earliest convenience. All other communication will be carried out by email.

You must complete and submit the questionnaire to us within 6 months of the order being processed. Any Questionnaire submitted after that date will not be assessed and no refund of the fees will be due or payable to you.

We will notify You of the results of our assessment as soon as reasonably practicable after completing its assessment.

If You are unsuccessful in your first assessment attempt, we will carry out one further assessment free of any additional charge provided that your resubmission is made within 48 hours of receipt of our notice that your first assessment attempt has failed. Any further assessment attempts will be charged as a new application.

Your submitted questionnaire must be complete and accurate in all material respects and has been completed honestly and in good faith.

The Cyber Essentials Plus must be completed within 3 months of completing the Cyber Essentials Self-Assessments completion.

If you are unsuccessful in your Cyber Essentials Plus assessment attempt, you have 30 days to remediate any issues internal or external or the assessment will have to be carried out again. All remediation must be complete within the 3-month allowance of completing the Cyber Essentials Self-Assessment else the whole assessment must be carried out. Any additional costs will be at the expense of your company.

We do not accept any liability to You resulting from any security breach or vulnerability in Your systems or processes either during the assessment or subsequently.

You must identify and disclose to us any third parties that may conceivably be affected by our testing activities, and any damages and/or loss of service caused by your failure to identify and/or disclose such third parties will remain your sole responsibility, and you therefore indemnify us against all and

any costs or damages howsoever arising from such activities. Your authorisation to commence testing activities is deemed to include confirmation that any relevant internal or external parties have been appropriately notified, and that all necessary permissions from such parties for us to commence testing have been provided to us.

We will only identify vulnerabilities that are already known at the date on which any tests are carried out, and which are capable of being exposed by the range of testing tools we deploy. You accept that it is technical security testing that there may be flaws that will be uncovered in the future or using alternative tools and attack methodologies, none of which could normally be identified at the time of testing, and you therefore agree that you will not, now or in the future, hold us to account for any such matters.

We will accept no liability for damages caused to you by any automated or non-automated attacks on your Internet-facing infrastructure or its applications, irrespective of whether our security testing activity carried out under this Agreement did, did not, or could have but did not identify any vulnerability exploited, or which might in future be exploited by any such attack.

We will issue the results of the Cyber Essentials Plus assessment as soon as reasonably practicable after completing its assessment. On completion of a successful assessment documentation will be emailed to the relevant contact with the certification, image, and branding agreement.

Vulnerability Assessment:

We will upon receipt of the Fees contact you within 24 hours (excluding weekends) of the order being processed and will, supply the request of all IP addresses to be scanned.

We do not accept any liability to You resulting from any security breach or vulnerability in Your systems or processes either during the assessment or subsequently.

You must identify and disclose to us any third parties that may conceivably be affected by our testing activities, and any damages and/or loss of service caused by your failure to identify and/or disclose such third parties will remain your sole responsibility, and you therefore indemnify us against all and any costs or damages howsoever arising from such activities. Your authorisation to commence testing activities is deemed to include confirmation that any relevant internal or external parties have been appropriately notified, and that all necessary permissions from such parties for us to commence testing have been provided to us.

We will only identify vulnerabilities that are already known at the date on which any tests are carried out, and which are capable of being exposed by the range of testing tools we deploy. You accept that it is technical security testing that there may be flaws that will be uncovered in the future or using alternative tools and attack methodologies, none of which could normally be identified at the time of testing, and you therefore agree that you will not, now or in the future, hold us to account for any such matters.

We will accept no liability for damages caused to you by any automated or non-automated attacks on your Internet-facing infrastructure or its applications, irrespective of whether our security testing activity carried out under this Agreement did, did not, or could have but did not identify any vulnerability exploited, or which might in future be exploited by any such attack.

We will issue the results of the vulnerability assessment as soon as reasonably practicable after completing its assessment. This will be available via a secure download portal for 30 days from the release.

Dark Web Scan:

We will upon receipt of the Fees contact you within 24 hours (excluding weekends) of the order being processed and will, supply the request of all domains to be scanned.

We do not accept any liability to You resulting from any security breach or vulnerability in Your systems or processes either during the assessment or subsequently.

We will issue the results of the Dark Web Scan as soon as reasonably practicable after completing its assessment. This will be available via a secure download portal for 30 days from the release.

Liability, Indemnity, and Insurance

The Service Provider shall ensure that it has in place at all times suitable and valid insurance that shall include public liability insurance.

In the event that the Service Provider fails to perform the Services with reasonable care and skill it shall carry out any and all necessary remedial action at no additional cost to the Client.

The Service Provider's total liability for any loss or damage caused as a result of its negligence or breach of the Agreement shall be limited to the sum defined therein.

The Service Provider shall not be liable for any loss or damage suffered by the Client that results from the Client's failure to follow any instructions given by the Service Provider.

Nothing in these Terms and Conditions nor in the Agreement shall limit or exclude the Service Provider's liability for death or personal injury.

The Client shall indemnify the Service Provider against any costs, liability, damages, loss, claims, or proceedings arising from loss or damage to any equipment (including that belonging to any third parties appointed by the Service Provider) caused by the Client or its agents or employees.

Neither Party shall be liable to the other or be deemed to be in breach of the Agreement by reason of any delay in performing, or any failure to perform, any of that Party's obligations if the delay or failure is due to any cause beyond that Party's reasonable control.

Force Majeure

No Party to the Agreement shall be liable for any failure or delay in performing their obligations where such failure or delay results from any because that is beyond the reasonable control of that Party. Such causes include, but are not limited to power failure, internet service provider failure, industrial action, civil unrest, fire, flood, storms, earthquakes, acts of terrorism, acts of war, governmental action or any other event that is beyond the control of the Party in question.

In the event that a Party to the Agreement cannot perform their obligations hereunder as a result of force majeure for a continuous period to be defined in the Agreement, the other Party may at its discretion terminate the Agreement by written notice at the end of that period. In the event of such termination, the Parties shall agree upon a fair and reasonable payment for all Services provided up to the date of termination. Such payment shall take into account any prior contractual commitments entered into in reliance on the performance of the Agreement.

Data Protection

The Service Provider will only use the Client's personal information as set out in the Service Provider's Data Handling Policy available from Red Circles ITS Limited.