TechForce™

Empowering your Cybersecurity

STATEMENT OF WORK
FOR
CYBER ESSENTIALS
&
CYBER ESSENTIALS PLUS

techforce.co.uk
ce@techforce.co.uk

Table of Contents

1. Introduction

This Statement of Work (SOW) outlines the agreement between _____ hereinafter referred to as the "Client," and TechForce Limited, hereinafter referred to as the "Service Provider," for the provision of cybersecurity certification services. The objective of this SOW is to define the scope, responsibilities, timeline, and deliverables for achieving Cyber Essentials and Cyber Essentials Plus certifications.

In this document, both parties mutually acknowledge their roles and responsibilities in the pursuit of enhancing the Client's cybersecurity posture and obtaining these prestigious certifications. The Client seeks to secure its digital assets and strengthen its resilience against common cyber threats, while TechForce, as the Service Provider, commits to assisting in achieving these cybersecurity milestones.

This SOW serves as a foundational document that governs the collaboration between the Client and TechForce, ensuring clarity and alignment in the pursuit of Cyber Essentials and Cyber Essentials Plus certifications.

2. Objectives

TechForce, hereinafter referred to as the "Service Provider," shall render cybersecurity certification services to the Client, with the aim of obtaining Cyber Essentials and Cyber Essentials Plus certification. The key objectives of this project are as follows:

2.1 Conduct a comprehensive evaluation of the Client's IT systems and network to ascertain compliance with the Cyber Essentials and Cyber Essentials Plus requirements.

2.2 Identify vulnerabilities, weaknesses, and areas necessitating enhancement within the Client's cybersecurity framework.

2.3 Aid the Client in executing essential cybersecurity controls to meet the certification criteria effectively.

2.4 Facilitate the certification procedure, including the a remote technical audit for Cyber Essentials Plus.

3. Scope of Work

3.1 Cyber Essentials Certification:

- The Service Provider shall collaborate with the Client to evaluate their existing cybersecurity measures against the Cyber Essentials framework.
- Recommendations for enhancements will be provided, and the Client shall be responsible for the implementation.
- The Service Provider will review and validate the applied controls to ensure compliance with the certification criteria.

Following successful adherence, the Service Provider will issue the Cyber Essentials certification.

3.2 Cyber Essentials Plus Certification:

- The Service Provider shall conduct a remote appraisal of the Client's IT systems and network to verify the control implementations.
- Vulnerability scanning and internal testing shall be conducted using Nessus Tenable Agents remotely.
- The Service Provider will also carry out Web browser test, file execution test, Anti-malware test, Email Security Configuration test, the assessor will also validate multi-factor authentication on the

client's Cloud Services and User accounts Separation using a remote desktop application called AnyDesk.

- Service provider then produces a Gap Analysis report along with the remediation advice if the client opted for Guided Cyber Essentials Plus package (CEP002). If not, a pass/fail report will be generated.
- It is the client's responsibility to remediate any identified issues.
- The service provider will perform a final audit.

Once the Client's security controls align with the Cyber Essentials Plus criteria, the Service Provider shall grant the Cyber Essentials Plus certification.

4. Timeline

The project timeline shall be mutually agreed upon by the Client and the Service Provider, incorporating significant milestones and deadlines for each milestone.

5. Deliverables

5.1 Preparation Phase

- Mutual Non-disclosure Agreement
- Vulnerability Assessment Authorization Form
- Pre-Vulnerability Questionnaire

5.2 Cyber Essentials Certification

- A comprehensive report detailing the assessment findings.
- Recommendations for improvement if it's the guided package (CEP002).
- Certification documentation upon successful compliance.

5.3 Cyber Essentials Plus Certification

- A detailed assessment report encompassing findings from the remote evaluation.
- Vulnerability assessment and testing reports.
- Gap analysis and remediation actions if it's the guided package (CEP002).
- Cyber Essentials Plus certification upon successful compliance.

6. Work Breakdown Structure

This outlines the detailed tasks and activities involved in performing a comprehensive Cyber Essentials Plus test. These tasks are organized to ensure a structured and systematic approach to the assessment.

6.1 Preparation

- Mutual Non-disclosure Agreement
- Vulnerability Assessment Authorization Form
- Pre-Vulnerability Questionnaire
- Cyber Essentials Questionnaire

6.2 Pre-Requisites

- Choosing the Sample for Vulnerability Scan (Assessor will choose & communicate)

- Installing Tenable Agents in the Sample Devices as per Assessor's guidelines
- Linking Tenable Agents to Tenable Cloud as per Assessor's Guidelines

6.3 Performing the Vulnerability Scan of the Sample

- Internal Scan
- External Scan

6.4 Performing the Host-based Audit

- Remotely connect with a set of sample devices
- Email Test (check email filters are in place)
- Browser Test (check browser blocks malware and is updated)
- Malware/AV-Test (check av gets triggered with flagged harmless malware)
- Multi-Factor Authentication (MFA) Test (verify if MFA is enabled for cloud services)
- Account Separation Test (verify if user account is used for day-to-day work and admin account is restricted)

6.5 If mobile devices are in scope, perform the following tests and provide evidence in the form of screenshots for each

- OS Support Check
- Ensure OS is Up-to-Date
- Verify Auto-Updates are Enabled
- Confirm the Device is not Jailbroken (Validate Trust Certificates Settings)
- Ensure the Device is Locked using a PIN/password

6.6 Final Report Submission and Cyber Essentials Plus Certificate Generation (done by Assessor)

- Compile and prepare the final assessment report
- Generating the Cyber Essentials Plus Certificate

Steps 6.3 & 6.4 will be repeated if the client has chosen the Guided package (CEP002).

7. Responsibilities

Both the Client and the Service Provider shall hold specific responsibilities throughout the certification procedure, including cooperation, data sharing, and the implementation of cybersecurity controls.

8. Costs

Quotation attached.

9. Payment Terms

The payment terms and associated fees for the Cyber Essentials and Cyber Essentials Plus certification services shall be explicitly defined in a separate agreement or invoice.

10. Confidentiality

Both parties are obligated to maintain the confidentiality of all information acquired during the project's course as stated in the Mutual Non-Disclosure Agreement that will be shared in the preparation phase

11. Termination

Both parties are obligated to maintain the confidentiality of all information acquired during the project's course as stated in the Mutual Non-Disclosure Agreement that will be shared in the preparation phase.

This Statement of Work shall be deemed binding upon endorsement by both the Client and the Service Provider. By appending signatures below, both parties confirm their understanding of, and compliance with, the terms and conditions outlined herein.

		TheTechForce Limited	
Signed		Signed	
Date		Date	
Name		Name	Jai Aenugu
Position		Position	Director

Terms and Conditions

Important: please read this carefully before accepting

Definitions:

- We, us, our, certification body – TheTechForce Limited, with registered office address at Balmoral Hub, Balmoral Park, Wellington Circle, Aberdeen. AB12 3J
- You, your - the person or organisation named as the client on the client application form.

The following terms apply to all purchases of Cyber Essentials and Cyber Essentials Plus:

- You must complete and submit the completed Cyber Essentials self-assessment questionnaire ('SAQ') on the IASME Consortium (IASME) portal ('Cyber Essentials Portal') within six months of placing the order. Any applications not completed within that period will be marked as void and your application will automatically be archived; in these circumstances, we cannot issue a refund and you agree that you will not be entitled to any refund of or reduction in the fee.
- If you require certification by a certain date, or before the expiry of an existing certificate, it is your responsibility to start the application in time to ensure it is completed before your deadline. In particular, you must provide an asset inventory and ensure that all assets, systems and applications that are within scope of a proposed certification are supported and meet the requirements of the Cyber Essentials scheme.
- We provide these services in accordance with the requirements of the IASME, which is the National Cyber Security Centre's ('NCSC') Cyber Essentials Partner for the delivery of the Cyber Essentials scheme, and we shall have no liability to you outside the scope of those requirements. From time to time, due to the ever-evolving nature of the cyber security sector, changes may be implemented by IASME or the NCSC. Such changes may cause price increases, which shall be passed on to you.
- If you are not successful on your first submission for Cyber Essentials, you will receive a 'More Information' or 'Fail' outcome. You then have two working days to submit a further attempt for certification. If you are not successful on your second submission, or if you fail to re-submit your second attempt within the two days, you will be required to purchase a new Cyber Essentials package and reapply.
- Before applying for Cyber Essentials Plus certification, you must confirm that you hold Cyber Essentials certification achieved through an IASME-licensed certification body within three months of applying.
- You will need to complete the Cyber Essentials Plus certification within three months of achieving your most recent basic-level Cyber Essentials certification. If your Cyber Essentials Plus application is unsuccessful, your Cyber Essentials certification may be revoked.
- For Cyber Essentials Plus applications, all scans including the internal and external vulnerability scans and the workstation assessment/technical audit must be completed and passed (including time to allow review by us in our capacity as the certification body) within a period of one month or within three months of the Cyber Essentials certificate, whichever date is earliest.
- If FOR ANY REASON you do not meet the deadlines outlined in the terms and conditions, then we will be under no obligation to provide the Cyber Services nor to refund any part of the agreed fee. Conversely, if we are required to do any additional work to help you complete your application, we may charge you separately for that work.
- For Cyber Essentials Plus applications, your explicit authorisation is required, as well as that from any additional parties involved in hosting any infrastructure or application that is in scope, before the start of any tests; this should be submitted in writing alongside the list of scan targets/IPs.
- Any limitations on the testing, such as a requirement for out-of-hours testing or weekend testing, or restrictions such as testing only during office hours, should be stipulated at the time of submitting the testing request. Any surcharges incurred for any out-of-hours testing will be agreed in advance and billed separately.
- If you fail any of the Cyber Essentials Plus testing performed as part of the overall engagement, we will

provide you with details of further tests required. The delay between the original assessment and retest should not exceed one month including completion of the application and including time to allow review by us (in our capacity as the certification body). These tests will be billed separately.

- Where we are required to provide on-site consultancy or testing at a customer site within or outside of the mainland United Kingdom, travel time and costs, accommodation and subsistence expenses may be chargeable. These expenses will be billed separately.
- Unless otherwise agreed, we reserve the right to list your name and/or logo on our website as evidence that certification has been achieved.
- Cancellations – we reserve the right to charge in full for booked days where you cancel with less than five business days' notice, and to charge 50% of the contracted rate where the day is cancelled between five and ten days in advance. In each case, we may waive the right to charge for a specific cancellation if we are able to deploy the consultant's time with an alternative client. We also reserve the right to charge (at cost) for any non-refundable expenses incurred in respect of travel and accommodation arrangements made in line with this agreement.
- If you are UK-domiciled, with a turnover under £20 million, and you achieve self-assessed certification covering your whole organisation to the basic level of Cyber Essentials, you are entitled to Cyber Liability Insurance (terms apply). The cover is underwritten by AXA XL, a division of AXA, and administered via Sutcliffe & Co. Insurance Brokers. This Cyber Liability Insurance does not form part of the agreement. Please visit https://iasme.co.uk/cyberessentials/cyberliabilityinsurance/.
- Both Cyber Essentials and Cyber Essentials certifications are valid for 1 year from the date of issue.
- We shall implement and maintain at all times during the term of the Statement of Work reasonable and appropriate administrative, technical and operational safeguards consistent with good industry practices and applicable law to ensure the security, confidentiality and integrity of all Confidential Information (as such term is defined in the Mutual Non-disclosure Agreement) including, without limitation, any Confidential Information obtained in connection with any access to your networks, computers or data. Without limiting the foregoing, we agree that we shall comply with all laws, regulations and secondary legislation, as amended or updated from time to time, including those relating to data protection, personal data and/or data privacy, that are applicable to us and our activities in connection with the Statement of Work. We will promptly (within seventy-two (72) hours) notify you if we become aware of any actual or suspected misuse, misappropriation, unauthorized disclosure, acquisition, loss, destruction, alteration, or corruption of Confidential Information ("Security Incident"). We will cooperate with you in order to investigate, remedy and/or resolve any such Security Incident, including, without limitation, in pursuing all legal remedies available to us or you, provided that we will not make any statements to any third party regarding such Security Incident without your prior written consent.
- We agree that in providing our applications and/or services we will not transmit any data that contains software viruses, time bombs, worms, Trojan horses, spyware, disabling devices, malicious code, or other harmful or deleterious computer code, files or programs to or through the applications and/or services.

Vulnerability scanning for Cyber Essentials Plus certification

- 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 in the nature of technical security testing that there may be flaws that will be uncovered in the future or by the use of 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 identify vulnerabilities that our testing has exposed and, wherever possible, we will identify by reference to commonly available and published information the appropriate patches and fixes that are

recommended to deal with the identified vulnerability, but it will be entirely your responsibility to formally identify and deploy an appropriate solution to the vulnerabilities identified by our security testing.

Guided products/services:

- Guided Cyber Essentials (CEB002) includes up to 2 hours of remote help to complete your questionnaire.
- Guided Cyber Essentials Plus (CEP002) includes the CEB002, Preaudits to highlight any gaps that need remediations before the final audit and up to an extra 2 hours remote support before your final audit.
- We can offer extra help at the additional cost if you need more help.