APPLICATION FORM – Cyber Essentials Mark or Cyber Trustmark

PART 1 - CONTACT DETAILS

a) Company Name:

b) Address:

Postal code:

c) Tel No: Fax No.:

d) Company Representative Name:

Title:

Contact No.:

Email:

PART 2 - COMPANY DETAILS

A. Company background

a) Scope of Activities to be Certified:

b) Company Registration No. (UEN Number):

c) Total number of employees:

d) Main reason for applying for certification:

e) Is your organization certified with any of the below schemes:

☐ ISO 27001: 2013

☐ Any Other Information or Cyber Security related Certifications:_____

f) If more than 1 site to be certified, please provide the below information (add lines accordingly):

	Company Name	Address	No. of Employees
Head Office			
Site 1			
Site 2			
Site 3			
Site 4			
Site 5			

PART 3 – IT Infrastructure

a) Brief Description of IT Infrastructure (Network – LAN/WAN, Servers, IT Security Devices, etc.):

b) Process and Tasks:

c) Do you share or outsource any IT Systems/Database/Telecommunication Systems (Yes/No)?
If Yes, please provide me the details:

PART 4 – Which tier of Cybersecurity Preparedness does my organisation belong to? (Only applicable for Cyber Trust Mark)

- ☐ Tier 1: Supporter
- ☐ Tier 2: Practitioner
- ☐ Tier 3: Promoter
- ☐ Tier 4: Performer
- ☐ Tier 5: Advocate

	Tier 1: Supporter	Tier 2: Practitioner	Tier 3: Promoter	Tier 4: Performer	Tier 5: Advocate
Cyber Governance and Oversight					
1. Governance			•	•	•
2. Policies and procedures			•	•	•
3. Risk management	•	•	•	•	•
4. Cyber strategy					•
5. Compliance	•	•	•	•	•
6. Audit				•	•
Cyber Education					
7. Training and awareness*	•	•	•	•	•
Information Asset Protection					
8. Asset management*	•	•	•	•	•
9. Data protection and privacy*	•	•	•	•	•
10. Backups*	•	•	•	•	•
11. Bring Your Own Device (BYOD)				•	•
12. System security*	•	•	•	•	•
13. Anti-virus/Anti-malware*	•	•	•	•	•
14. Secure Software Development Life Cycle (SDLC)					•
Secure Access and Environment					
15. Access control*	•	•	•	•	•
16. Cyber threat management				•	•
17. Third-party risk and oversight					•
18. Vulnerability assessment			•	•	•
19. Physical/environmental security		•	•	•	•
20. Network security		•	•	•	•
Cybersecurity Resilience					
21. Incident response*	•	•	•	•	•
22. Business continuity/disaster recovery		•	•	•	•
	10 DOMAINS	13 DOMAINS	16 DOMAINS	19 DOMAINS	22 DOMAINS

*Measures in Cyber Essentials mark