Cyber Essentials

Common Questionnaire

V1.1

This document has been prepared with the assistance of the IASME Consortium Ltd and CREST (GB) Ltd, and is derived from work carried out by those organisations under contract to HMG (BIS, CESG, Cabinet Office) during the development of the Cyber Essentials Scheme

Version Control

Version	Date	Description	Released by
1.0	07/08/14	Initial Common Questionnaire	SR Smith
1.1	23/09/14	Error correction, introduced footer version	SR Smith

Introduction

The Cyber Essentials scheme is recommended for organisations looking for a base level Cyber security test where IT is a business enabler rather than a core deliverable. It is mainly applicable where IT systems are primarily based on Common-Off-The-Shelf (COTS) products rather than large, heavily customised, complex solutions.

The main objective of the Cyber Essentials assessment is to determine that your organisation has effectively implemented the controls required by the Scheme, in order to defend against the most common and unsophisticated forms of cyber attack.

This questionnaire is a self assessment, which must be approved by a Board member or equivalent, and which will be verified by a competent assessor from the Certifying Body. Such verification may take a number of forms, and could include, for example, a telephone conference, or a vulnerability scan. The verification process will be at the discretion of the Certifying Body.

Please note that Certifying Bodies are not required to use this questionnaire, and may have developed an alternative form. This is acceptable with the parameters of the Scheme, and any variation to the questionnaire will have been approved by the Scheme Authority as providing at least the same level of assurance.

Scope of Cyber Essentials

The Scope is defined in the scheme Assurance Framework document, available on the scheme web site https://www.cyberstreetwise.com/cyberessentials/#downloads

You will be required to identify the actual scope of the system(s) to be evaluated as part of the questionnaire.

Organisation Identification

Please provide details as follows:

Organisation Name (legal entity):	
Sector:	
Parent Organisation name (if any):	
Size of organisation (Micro/SME/Large etc)	
No of employees	
Point of Contact name:	
Job Title:	
Email address:	
Telephone Number:	
Certifying Body (CB):	
CB Reference number:	

Business Scope

Please identify the scope of the system(s) to be assessed under this questionnaire, including locations, network boundaries, management and ownership. Where possible, include IP addresses and/or ranges.

A system name should be provided that uniquely identifies the systems to be assessed, and which will be used on any certificate awarded. *(Note: it is not permissible to provide the company name, unless all systems within the organisation are to be assessed):*

Boundary Firewalls and Internet Gateways

	Question	Answer	Comment
1	Have you installed Firewalls or similar devices at the boundaries of the networks in the Scope?	*Always* *Mostly* *Sometimes* *Rarely* *Never*	
2	Have the default usernames/passwords on all boundary firewalls (or similar devices) been changed to a strong password	*Always* *Mostly* *Sometimes* *Rarely* *Never*	
3	Have all open ports and services on each firewall (or similar device) been subject to justification and approval by an appropriately qualified and authorised business representative, and has this approval been properly documented?	*Always* *Mostly* *Sometimes* *Rarely* *Never*	
4	Have all commonly attacked and vulnerable services (such as Server Message Block (SMB) NetBIOSm tftp, RPC, rlogin, rsh, rexec) been disabled or blocked by default at the boundary firewalls?	*Always* *Mostly* *Sometimes* *Rarely* *Never*	

5	Confirm that there is a corporate policy requiring all firewall rules that are no longer required to be removed or disabled in a timely manner, and that this policy has been adhered to (meaning that there are currently no open ports or services that are not essential for the business)?	*Policy exists and has been implemented* *Policy exists but has not been implemented* *Policy does not exist*	
6	Confirm that any remote administrative interface has been disabled on all firewall (or similar) devices?	*Always* *Mostly* *Sometimes* *Rarely* *Never*	
7	Confirm that where there is no requirement for a system to have Internet access, a Default Deny policy is in effect and that it has been applied correctly, preventing the system from making connections to the Internet	*Always* *Mostly* *Sometimes* *Rarely* *Never*	

Please provide any additional evidence to support your assertions above:

Secure Configuration

	Question	Answer	Comment
8	Have all unnecessary or default user accounts been deleted or disabled	*Yes* *No*	
9	Confirm that all accounts have passwords, and that any default passwords have been changed to strong passwords?	*Always* *Mostly* *Sometimes* *Rarely* *Never*	
10	Has all unnecessary software, including OS utilities, services and applications, been removed or disabled	*Always* *Mostly* *Sometimes* *Rarely* *Never*	
11	Has the Auto Run (or similar service) been disabled for all media types and network file shares?	*Always* *Mostly* *Sometimes* *Rarely* *Never*	

12	Has a host based firewall been installed on all desktop PCs or laptops, and is this configured to block unapproved connections by default?	*Installed and configured* *Installed, but not configured* *Not installed*	
13	Is a standard build image used to configure new workstations, does this image include the policies and controls and software required to protect the workstation, and is the image kept up to date with corporate policies?	*Yes* *No*	
14	Do you have a backup policy in place, and are backups regularly taken to protect against threats such as ransomware?	*Yes* *No*	
15	Are security and event logs maintained on servers, workstations and laptops?	*Yes* *No*	

Please provide any additional evidence to support your assertions above:

Access Control

	Question	Answer	Comment
16	Are user account requests subject to proper justification, provisioning and an approvals process, and assigned to named individuals?	*Yes* *No*	
17	Are users required to authenticate with a unique username and strong password before being granted access to computers and applications?	*Yes* *No*	
18	Are accounts removed or disabled when no longer required?	*Yes* *No*	
19	Are elevated or special access privileges, such as system administrator accounts, restricted to a limited number of authorised individuals?	*Yes* *No*	
20	Are special access privileges documented and reviewed regularly (e.g. quarterly)?	*Yes* *No*	
21	Are all administrative accounts only permitted to perform administrator activity, with no Internet or external email permissions?	*Yes* *No*	
22	Does your password policy enforce changing administrator passwords at least every 60 days to a complex password?	*Yes* *No*	

Please provide any additional evidence to support your assertions above:

Malware Protection

	Question	Answer	Comment
23	Please confirm that malware protection software has been installed on at least all computers with an ability to connect outside of the network in Scope	*Always* *Mostly* *Sometimes* *Rarely* *Never*	
24	Does corporate policy require all malware protection software to have all engine updates applied, and is this applied rigorously?	*Yes* *No*	
25	Have all malware signature files been kept up to date (through automatic updates or through centrally managed deployment)?	*Yes* *No*	
26	Has malware been configured for on-access scanning, and does this include downloading or opening files, opening folders on removable or remote storage, and web page scanning?	*Yes* *No*	
27	Has malware protection software been configured to run regular (at least daily) scans?	*Yes* *No*	
28	Are users prevented from running executable code or programs form any media to which they also have write access?	*Always* *Mostly* *Sometimes* *Rarely* *Never*	

29	Are users prevented from accessing known malicious web sites by your malware protection software through a blacklisting function?	*Yes* *No*	

Please provide any additional evidence to support your assertions above:

Patch Management

	Question	Answer	Comment
30	Is all software installed on computers and network devices in the Scope licensed and supported?	*Always* *Mostly* *Sometimes* *Rarely* *Never*	
31	Are all Operating System security patches applied within 14 days of release?	*Always* *Mostly* *Sometimes* *Rarely* *Never*	
32	Are all Application software security patches applied within 14 days of release?	*Always* *Mostly* *Sometimes* *Rarely* *Never*	
33	Is all legacy or unsupported software isolated, disabled or removed from devices within the Scope?	*Yes* *No*	
34	Is a mobile working policy in force that requires mobile devices (including BYOD) to be kept up to date with vendor updates and app patches?	*Yes* *No*	

Please provide any additional evidence to support your assertions above:

Approval

It is a requirement of the Scheme that a Board level (or equivalent) of the organisation has approved the information given. Please provide evidence of such approval: