Cyber Essentials Scheme

Applicant: IL7,

Thank you for applying for certification to the Cyber Essentials Scheme Self-Assessment.

Congratulations, you have been successful.

I include below the results from the form which you completed.

Question	Answer	Assessor score	Comments
Does the scope of this assessment cover your whole company?	Yes I am a single user of my IT. The scope includes my laptop, my PC at home (with printer) and a further desktop that I use solely for CESG IS1 risk assessments, plus an external hard drive I use for encrypted backups). And a USB storage device with encryption.	Compliant	
Please describe the locations of your business which are in the scope of this assessment	My home office. A secure converted bedroom I can lock and is locked. No one else has access. There is a lockable cabinet where I store any customer documents.	Compliant	
Please describe the information systems which are in the scope of this assessment	One Desktop - OS Win 10, Applications MS Office, Adobe One Laptop OS Win 10, MS Office One Desktop Win 7 Used for Documents - word. Non classified unless I used encrypted drive and then no higher than OFFICIAL, Also do Excel spreadsheets and PowerPoint presentations, Visio drawings - access web for research and internet banking. Email for correspondence and assignments.	Compliant	

Question	Answer	Assessor score	Comments
Please describe the boundary of the networks that will be in the scope for this assessment	None of my machines are networked. All have WiFi access. I have a mobile EE Router and a router at home provided by SKY. IL7 do not have Ethernet to any other networks except the Internet , There are three computers are used which are in scope. My laptop which I bring down to the hotel wherever I am based (currently Abbey Wood, before that BAE in Barrow, before that London with the Passport Office etc.)The laptop can access the Internet – I have my own EE provided hub (I avoid hotel internet and 'the cloud') but sometimes use the AW hotspot. At home I use the router installed by SKY with the broadband – my partner had it installed before I arrived. At home I also have a desktop on which I have Windows 10, and that uses the SKY router also. I have a third machine which is the only one I can get the IS1 tool (which customers still like, while I prefer the hand cracking method) to work on. On firewalls, I have installed, set up the rules, reviewed many (industrial sized) firewalls. At DERA in the nineties, I was the grade 7 in charge of developing all the networks (I invented CORNET and ICE). I wrote the configuration guide for the very first firewall in the MOD, a TIS (Trusted Information Systems) Gauntlet Firewall – and got it certified through CLEF. In those days we in Malvern hosted the CESG web site and the queen sent	Compliant	

Question	Answer	Assessor score	Comments
	her first email from L Block ya de ya……!. So yes if I had a stand-alone office firewall it would be set up with a white list, it would deny certain services etc. Back in the days I would be talking Memo 13, Manual M, N, & P but now I would be using whatever GPG was relevant. Essentially, nowadays, I would use it to the manufacturers recommendations filtered by the circumstances. But anyway the scope of the exercise means I don't think I need one. There are personal firewalls and AV on all machines – the risk assessment on IL7 is summarised thus – information assets minimal (Very little customer data, some personal and some financial data), potential threat actors include myself, my partner, visitors to the house and hackers (motivation minimal, capability limited (by means of access control, encryption, personal firewall etc). The IL1 tool churns out only very low risks.		
Who is responsible for managing the information systems in the scope of this assessment?	Joe Ferguson. SC cleared, previously DV. Head Consultant, CLAS, SIRA Senior Practitioner, CCP, Full member of the IISP. Any technical issues that I cannot handle I refer out to Michael Ferguson, CCISP, MCE. Joe Ferguson 07817689081	Compliant	
Please provide your company name (*as it is registered with Companies House*)	IL7 Ltd (reg. 7927451)	Compliant	
Please provide your company address (*as it is registered with Companies House*)	10 Walpole Gardens, Chiswick, London W4 4HG.	Compliant	

Question	Answer	Assessor score	Comments
What is your main business?	Information and communication Information Assurance. IA Risk Assessment and Cyber Compliance. I am a CLAS consultant. I do work mainly for HMG and Police Forces. I work for the most part on customer premises providing IA advice and documentation to HMG standards. I sometimes receive work at home via CJSM but nothing above OFFICIAL.	Compliant	
What is your website address?	www.IL7security.com This is currently being rebuilt by Michael Ferguson	Compliant	Website appears to have a number of paged that have place holder content
Is your organisation domiciled in the UK?	Yes Patrick Ferguson, Director and Company Secretary resides at the company HQ in London and manages IL7 finances and company business. I live in Birmingham though I presently work with the MOD in Bristol and commute on a weekly basis. Prior to that I was working for BAE in Barrow on Furness, a weekly commute also.	Compliant	
Is your gross annual turnover **less than** £20m?	Yes Its average over the past three years has been £120,000 pa	Compliant	

Question	Answer	Assessor score	Comments
Your company is eligible for the included cyber insurance if you gain certification. If you do not want this insurance element please opt out here. The cost of this is included in the assessment package and you can see more about it here. Would you like to take out the cyber insurance policy?	Yes	Compliant	
What is your total gross revenue? The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification	£130,000 pa	Compliant	
Is the company or its subsidiaries any of the following: medical, call centre, telemarketing, data processing (outsourcers), internet service provider, telecommunications or an organisation regulated by the FCA? The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification	No But I do have £2 million personal indemnity. Updated in line with CESG Cyber	Compliant	
Does the company have any domiciled operation or derived revenue from the territory or jurisdiction of Canada and / or USA? The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification	No	Compliant	
What is the size of your business? *According to the EU definition of a Small and Medium-sized Enterprise (SME)*	Micro (<10 Employees and <€2m Turnover)	Compliant	

Question	Answer	Assessor score	Comments
How many staff regularly work from home?	1 I sometimes work on non-customer information that is relevant to my work from home. In the past I have taken assignments to produce papers at home. I have used the customers encrypted VPN and my own disk encryption. There is no remote access.	Compliant	
Do you ensure that your system does not contain valid accounts which are not used?	Yes Guest accounts are disabled. All accounts are password protected as well as having lock down on the screen savers.	Compliant	
Is access to information restricted to authorised users who have a bona-fide business need to access the information?	Yes Only Joe Ferguson has access to customer data. Only Patrick Ferguson has access to accounts.	Compliant	
Have you changed the default passwords which came with your router and other devices?	Yes All device passwords have been changed. The router password is known only to Joe Ferguson	Compliant	
Are all users required to use two-factor authentication to log in to access terminals? *Note that username and password do not fall with in the definition of two-factor authentication, which is usually defined as something you know (e.g. username and password) and something you have (e.g. a token) or something you are (e.g. fingerprint, retinal and/or facial recognition).*	No Not necessary. To access bank details this is required but not standard access. This would be implemented for remote access	Compliant	Two factor authentication would add an extra layer of security. It is appreciated it can be a large undertaking to roll out across the board, but it is recommended you start on a risk prioritised basis. Home and mobile working solutions are often selected first for the extra risk associated. This would seem an appropriate starting point in your case for having a remote working solution.

Question	Answer	Assessor score	Comments
Do you control remote access to your system?	Yes Not Applicable for users. There is no access enabled so it cannot be exploited.	Compliant	
Do you have a formal policy for giving someone access to systems at an “administrator” level?	Yes Only Joe Ferguson has administrator access.	Compliant	
Have you changed the administrative password on all your devices and networks to a strong password? *A strong password typically is a mixture of at least 8 characters, numbers and symbols, the longer the better.*	Yes AS per policy. Il7 passwords are more complex than the advice given here. They are CESG compliant to the required entropy.	Compliant	
Do any of your staff work on a day-to-day basis with a user account with administrative privileges?	No Joe Ferguson uses his own account unless reconfiguring or updating software.	Compliant	
Do you have a list of the people who have administrator accounts in your company?	Yes It is contained in the S&DPG. The only admin is Joe Ferguson.	Compliant	
Is the list of the people who have administrator accounts kept in a secure location? *Such as a safe or encrypted file*	Yes IL7 has recently changed this policy in respect to a threat to availability rather than confidentiality. Both Patrick and Michael are in receipt of an encrypted file containing Joe Ferguson's administrator password. They both know their own password to unlock the encryption key. They are responsible for keeping this encrypted on a personal CD stored safely.	Compliant	

Question	Answer	Assessor score	Comments
Do you review who should have administrative access on a regular basis?	Yes This was only changed recently with regard to the previous submission. I have considered giving Michael permission for technical access but this has not been done. We have it as an agenda item for the Quarterly meeting.	Compliant	
When was the last time you reviewed who had administrative access?	7 12 15. Yesterday. It will be on the agenda in February and quarterly afterward.	Compliant	
Do you change the passwords on your administrative accounts at least every 60 days?	Yes This is every thirty days.	Compliant	
How do you remember to change the passwords on your administrative accounts?	Other [Specify In Notes Field] This is a task for Joe Ferguson on 1st day of each month and included in the S&DP User Passwords are changed it as frequently as asked to change the password on the customers system. This has become a habit over the years.The maximum for admin accounts is 30 days.	Compliant	
Do you ensure that none of your users and administrators have the same account names?	Yes All accounts are unique. Joe Ferguson user account has no administrative privileges.	Compliant	

Question	Answer	Assessor score	Comments
Can you only access applications, computers and network devices in your company by entering a unique user name and password?	Yes Each account is unique and password protected. There was an account on the PC for my fiancé but no access to documents or applications unique to Joe Ferguson account or the Administrator account. Her account has now been deleted and she has no access to the PC.	Compliant	
Do all your users and administrators use strong passwords? *A strong password typically is a mixture of at least 8 characters, numbers and symbols, the longer the better.*	Yes There is only one administrator, Joe Ferguson and the password is 12 characters, four triplets made up of lower/upper case, numbers and special character. User accounts ate 8 characters and a mix of lower upper case characters, numbers and at least one special character. They are deliberately hard to guess but easy to remember containing no associational references (football teams/pets/real names etc)	Compliant	
Have you deleted, or changed the password on, any accounts for staff who are no longer with your company? *When an individual leaves your organisation you need to stop them accessing any of your systems.*	Yes When Michael left for Australia, his account and password and all files were deleted,	Compliant	
Do you ensure that staff do not have privileges that they do not need to do their current job? *When a staff member changes job role you may also need to change their access privileges.*	Yes This is recognised in the S&DPG. IL7 recognise the principle of least privilege and	Compliant	

Question	Answer	Assessor score	Comments
Have you removed all the software your devices came with but which you do not need?	No This is a mixed bag. Much of it has only been installed because I need it but there is some left on because it may be needed.The PC has not been subject to GAP.	Compliant	Accepted but if software is not used it should be removed to reduce attack surface and patch burden
Have you removed all other software which you do not need or use?	Yes Windows now comes with so much it is difficult to know what to uninstall without getting expert help in and that might compromise something else.	Compliant	
Have you disabled all auto-run programmes on your systems? *Often there is a setting which automatically runs programmes when CDs/DVDs/memory sticks etc. are inserted. This is not secure as you or your anti-malware software should review a programme before the computer runs it in case it is malware. You can disable this auto-run feature through the control panel / system preferences.*	Yes	Compliant	
When was the last time you had a vulnerability scan on your system?	The last MBSA was today (10.12.15) Microsoft Baseline Security Analyser is on all machines and used to scan every week. I run spy a spy bot scan each week. Avast AV runs continuously as does Spy bot and the Avast and Microsoft Firewalls. I also try out free/share ware eval copies so my scans are more frequent..	Compliant	Running an anti-virus scan is not the same as running a vulnerability scan. This is something which will provide a good view of the potential vulnerabilities within your organisation and across all devices on the network. It is difficult to manage your technical security without it. A tool such as MBSA would be a good start

Question	Answer	Assessor score	Comments
Did you act to improve the security of your system on the basis of the scan results?	Yes I always clean up problems. I do not just quarantine them. Discovered applications loaded when upgrade to Win 10 did not have secure passwords and acted upon these.	Compliant	
Are all the operating systems on your devices supported by a supplier which sends you regular fixes for any problems?	Yes MS updates automatically Avast AV frequently asks to be updated and this gets done. Spy bot is similar but less frequent.	Compliant	
Are all the applications on your devices supported by a supplier which sends you regular fixes for any problems?	Yes See above.	Compliant	
Are systems hardware, firmware and software licensed in accordance with the publisher's recommendations?	Yes	Compliant	
How do you know when there is a new update for your software?	Updates automatically AS above - its a mixture. Most send notifications. MS is automatic if connected to the Internet.	Compliant	
Do you believe that all the software you use is up to date?	Yes As much as can be. Trucrypt was discontinued but still work and as far as I am concerned is still fit for purpose. It was only broken in Lab conditions and the data I might encrypt is OFFICIAL at the highest.	Compliant	
Are your computers set to automatically install software updates?	Yes Part. Microsoft and AV. All others I do on an as and when needed basis.	Compliant	

Question	Answer	Assessor score	Comments
Have you installed all the latest software patches on all your devices?	Yes As far as I know.	Compliant	
Do you update software when new versions are released?	Yes Mostly (see above)	Compliant	
Have you installed anti-malware software on all your computers and laptops in scope?	Yes Windows 10 uses built in Windows Defender. Default Settings used. Spy bot and Avast AV run continuously.	Compliant	
Is the anti-malware software on your computers and laptops set to update itself automatically?	Yes Windows 10 uses built in Windows Defender Avast asks but always gets updated.	Compliant	
Is the anti-malware software on your computers and laptops set to scan files automatically upon access (including when downloading and opening files, accessing files on removable storage media or a network folder) and scan web pages when being accessed via a web browser?	Yes Windows 10 uses built in Windows Defender Automatic	Compliant	
Is the anti-malware software on your computers and laptops set up to perform regular scans of all files daily?	No JF runs scans daily when possible. PC switched off when away from home office.	Compliant	Accepted
Does the anti-malware software on your computers and laptops prevent you or warn you about connecting to suspicious websites?	Yes	Compliant	

Question	Answer	Assessor score	Comments
Do you run anti-malware software at least daily against all stored data?	Yes See above. On the Laptop. When Joe Ferguson is working away from home the PC is switched off. Once switched on it scans and updates. Both have Windows Defender with Windows 10.	Compliant	
Does the anti-malware software examine data and applications each time they are used?	Yes Windows 10 has Windows Defender. It automatically runs in the background.	Compliant	
Do you, or any of your staff, use tablets or smart phones for business purposes?	No Phone are for calls mainly. Yes I use the camera on occasion, maps, banking, and the satnav and some other apps (google to finish the Times crossword sometimes). I don't access facebook or any other social websites.	Compliant	
Do you use firewalls or (something similar) to protect your systems and devices from outside threats?	Yes I use Avast Firewall on all machines. The Windows Firewall is also on each machine.	Compliant	
When you first receive an office firewall it will have had a default password on it. Has this initial password been changed?	Yes	Compliant	A firewall is necessary but in this case home and office are the same thing
Is the new password on your office firewall a strong one? *A strong password typically is a mixture of at least 8 characters, numbers and symbols, the longer the better.*	Yes It is CESG compliant with strong entropy. It is made up of four couplets.	Compliant	

Question	Answer	Assessor score	Comments
Do you know what kind of files your office firewall allows through from the internet to your system?	Yes Only allows files requested. Firewalls set to default.	Compliant	
Have you or someone else who manages your IT system set the rules on your office firewall to allow some traffic through and block other traffic?	Yes Set to default which does not allow suspicious files.	Compliant	
Have you, or has one of your service providers, blocked services on your office firewall which are generally considered to be vulnerable? *There are some services which are typically more vulnerable to attack than others and you would probably need to block these at your office firewall. These include services such as Server Message Block (SMB), NetBIOS, tftp, RPC, rlogin, rsh or rexec. Some IT systems will need one or more of these to operate and it will be a business decision about whether to block that service or not.*	Yes Set by default.	Compliant	
Do you have a business case for the vulnerable services which are not blocked on your firewall?	Yes I believe all vulnerable services are blocked. I have now looked at creating a business case file for logging any time pop ups required by an application. For example I had to temporarily allow pop ups in order to access the Cabinet Office online tendering forms for CESG.application.	Compliant	

Question	Answer	Assessor score	Comments
Do you currently have any extra services enabled on your office firewall which are not now required? *At times your office firewall may be configured to let a certain kind of service through so you can operate an aspect of a project or part of your business. If circumstances change or that project comes to an end you should reconfigure your office firewall to a more secure setting once you do not need that service any more. You should review the configuration of your firewall regularly to ensure that all extra services which had to be enabled before, but are not now needed, have been re-set to the safer mode.*	No The personal firewalls for which Firewall rules were relaxed to allow pop ups have now been put back to the previous settings.	Compliant	
Do you change the password regularly?	Yes At the same time that the admin password.is changed - minimum of 30 days..	Compliant	
Does any other person or organisation have access to your firewall administrative account over the internet?	No Joe Ferguson has sole admin access.	Compliant	
Have all the answers provided in this assessment been approved at Board level or equivalent?	Yes This is Patrick. We have discussed and I agree with the information provided. I have read the revised S&DPG and this is now signed off. Patrick is on 07860779816	Compliant	
Has the attached Cyber Insurance Declaration been downloaded (by clicking here), completed and signed (by a Board level or equivalent signatory), then uploaded (using the function provided below)?	Yes	Compliant	

Certificate of Assurance

IL7 Ltd (reg. 7927451)

10 Walpole Gardens, Chiswick, London W4 4HG.

Scope: Whole Company

Complies with the requirements of the Cyber Essentials Scheme

Date of Certification: 13th December 2015
Recertification Due: December 2016
Certificate Number: IASME-A-00560
Profile Published: April 2014

Certification Body: baigent's Information Security Services ltd

Assessor: Jon Baigent

Accreditation Body: IASME Consortium

This Certificate certifies that the organisation named was assessed as meeting the Cyber Essentials implementation profile published in April 2014 and thus that, at the time of testing, the organisations ICT defences were assessed as satisfactory against commodity based cyber attack. However, this Certificate does not in any way guarantee that the organisations defences will remain satisfactory against cyber attack.