Home Working / Own Device Use Compliance Checks and Signoff

INTRODUCTION

Hello,

We've put together this checklist that is design for two purposes; to keep your company data secure and to aid compliance to the Cyber Essentials standard for staff / freelancers / associates when they are using their own devices to access your systems.

With the rise of home / remote working you loose the control of the security of your business data, even more so if you allow your staff or other workers access to this data from their own devices.

- Where is the data held?
- What protection does it have on it?
- Is it being updated with software patches when needed?
- How can I control access to my business data?

The best way to control your business data is to own the device that the data is accessed from, as you have complete control of the security settings and data retention. However that is not always practical and that's why we have created this checklist and employee / freelancer / assocaite sign off form for your business.

This checklist outlines all the cyber essentials requirements, and these are the same if a device is company owned or otherwise. There is also a sign off form you can issues to people who user their own devices to say they have understood the data security requirements of them to work with you and your data.

If you have any questions, just let us know.

Speak Soon,

Michael Freeman

Michael Freeman
CyberEssentials@SouthernIT.com
01323 287828

PS – It takes just one device, or weak password to compromise your entire company, don't be tempted to just ignore it

Southern IT Networks are a Certification Body for the NCSC Cyber Essentials Scheme. The Accreditation partner for the NCSC is IASME and a complete list of certification bodies can be found on their website at https://iasme.co.uk/certification-bodies/

CONTENTS

PASSWORD POLICIES

Requirements

All passwords I use meet or exceed the following requirements:

- ☐ Minimum of 8 characters (13 Characters plus is best practice)
- ☐ Must Include upper and lower case letters
- ☐ Must Include special characters (i.e. $ % ! >)
- ☐ Must not be easily guessable such as Password123
- ☐ Must not include identifiable words (children's names, sports clubs) or any company name

Internet Router / Firewall

Requirements

Where a Business VPN is used, this requirement can be taken out of scope.

- ☐ Make and model of your internet router: _____

  (This is usually printed on a label on the back of your internet router.)

- ☐ I do not publish any services to the internet from inside my network.

  (For example, some people publish their CCTV system at home to the internet so they can connect to it remotely If you don't do anything like this then please confirm you don't. If you do please list the details for us to review.)

- ☐ I Have changed the default password on my Internet Router

  (even though passwords on most newer home routers are seemingly random, they are not, and still require changing to meet the password requirements above)

Computers (PC's or Mac)

Requirements

- ☐ List Operating System and Version: _____

  (e.g. Windows 10 Pro 1909)

- ☐ I do not operate day to day usage of my device as an 'Administrator'

  (For most home PC's people operate as an administrator, and in doing so run a much higher risk of malware or viruses doing serious harm as they can operate with the same rights you are logged in with, when logged in as a standard user, the malware or virus may be mitigated or the spread contained. A good test of whether you operate as an administrator is if you can install software with the account, then it has admin privileges, and you should create a secondary account for the admin, and downgrade your current one to a standard user.)

- ☐ I have removed all unused software.

If software is unused but, on a device, it represents an area that could be used for an attack, but removing unused software, you reduce the 'attack surface'

- ☐ I have enabled the firewall on my computer.
- ☐ Auto run / Auto play is disabled.

  Turning Off the auto run / auto play functions means that media inserted to the device can not automatically deploy malicious software.

- ☐ All applications I use are supported by the vendor and licensed where required.

  If an application is no longer support by the vendor, then there are also not security updates for it, and as time goes on, the risk of attack becomes greater.

- ☐ I install all high and critical firmware and software updates within 14 days of release.
- ☐ All applications are removed when they become unsupported by the vendor or not required
- ☐ I use two factor authentication for all administrator accounts on systems I use where its available.
- ☐ I have antivirus software installed, running and its always updated.
- ☐ My antivirus / anti Malware program also scans websites

Mobile Phones

If you intend to access emails, chat or any other company data on your mobile phone please implement the following requirements.

Requirements

- ☐ List Phone Make / Model& Operating System: _____

  (e.g. iPhone X running iOS 13)

- ☐ I have enabled a pin lock code which is at least 8 characters long.

  Biometrics logins can still be used (Face ID and Fingerprint) but the pin code / password should be 8 characters / digits.

- ☐ I have secured my device against malicious programs by:
  (Typically for mobile devices the b. option below is used, rather than antivirus)

- ☐ A) Installing antivirus software which is running and its always updated.
- ☐ B) Only installing applications from the official app store OR from a list of apps that have been approved by the company.

- ☐ I have removed all unused applications.
- ☐ I install all Critical and High security and software updates within 14 days of release.
- ☐ All programs get removed when they become unsupported by the vendor or unused.
- ☐ I confirm that I have not 'jailbroken' or 'rooted' my device

Acceptance and Sign Off

Full Name: _____

Role: _____

Date: _____

I confirm that:

- I have implemented all the requirements as outlined in this document
- I will allow full access to our IT Provider and Certification Body to perform checks on my devices as required for the Cyber Essentials requirements to verify this.
- I will continually check my devices remain in compliance of the Cyber Essentials Certification Requirements.
- I will inform you as soon as possible after any event that may breech the security of my devices or your business data.
- I will implement any new measures required in the future by the Cyber Essentials standard.

Signature: _____