CYBER ESSENTIALS UPDATES 2022

HOME WORKING DEVICES ARE IN SCOPE, BUT MOST HOME ROUTERS ARE NOT.

Anyone working from home for any amount of time is classified as a 'home worker'. The devices that home workers use to access organisational information, whether they are owned by the organisation or the user, are in scope for Cyber Essentials.

Home routers that are provided by Internet Service Providers or by the home worker **are now out of scope and the Cyber Essentials firewall controls are now transferred to the home worker's device (computer, laptop, tablet and/or phone).** However, a router supplied by the applicant company is in scope and must have the Cyber Essentials controls applied to it.

The use of a corporate (single tunnel) Virtual Private Network (VPN) transfers the boundary to the corporate firewall or virtual cloud firewall.

ALL CLOUD SERVICES ARE IN SCOPE

Cloud services are to be fully integrated into the scheme. If an organisation's data or services are hosted on cloud services, such as AWS or MS Azure then the organisation is responsible for ensuring that all the Cyber Essentials controls are implemented.

Whether the cloud service provider or the user implements the control, depends on the type of cloud service.

MULTI FACTOR AUTHENTICATION MUST BE USED FOR ACCESS TO CLOUD SERVICES

As well as providing extra protection for passwords that are not protected by other technical controls, multi factor authentication should always be used to provide additional protection to administrator accounts and accounts when connecting to cloud services.

The password element of the multi-factor authentication approach must have a password length of at least 8 characters with no maximum length restrictions.

THIN CLIENTS ARE IN SCOPE WHEN THEY CONNECT TO ORGANISATIONAL INFORMATION OR SERVICES

A thin client is a 'dumb terminal' that gives you access to a remote desktop. It doesn't hold much data, but it can connect to the internet.

ALL SERVERS INCLUDING VIRTUAL SERVERS ON A SUB-SET OR A WHOLE ORGANISATION ASSESSMENT ARE IN SCOPE

Servers are specific devices that provide organisational data or services to other devices as part of the business of the applicant.

December 2021

DEFINITION OF A 'SUB-SET' AND ITS IMPACT ON SCOPE

A sub-set is defined as a part of the organisation whose network is segregated from the rest of the organisation by a firewall or VLAN. A sub-set can be used to define what is in scope or what is out of scope of Cyber Essentials. Use of individual firewall rules per device are no longer acceptable.

DEFINITION OF 'LICENSED AND SUPPORTED'

Licensed and supported software is software that you have a legal right to use and that a vendor has committed to support by providing regular patches or updates. The vendor must provide the future date when they will stop providing updates. The vendor does not have to be the original creator of the software, but they must have the ability to modify the original software to create updates.

ALL SMART PHONES AND TABLETS CONNECTING TO ORGANISATIONAL DATA AND SERVICES ARE CONFIRMED IN SCOPE WHEN CONNECTING TO CORPORATE NETWORK OR MOBILE INTERNET SUCH AS 4G AND 5G.

However, mobile or remote devices used only for voice calls, text messages or multi-factor authentication applications are out of scope.

DEVICE LOCKING

Biometrics or a minimum password or pin length of 6 characters must be used to unlock a device.

PASSWORD-BASED AND MULTI-FACTOR AUTHENTICATION REQUIREMENTS

When using passwords, one of the following protections should be used to protect against brute-force password guessing:

- Using multi-factor authentication
- Throttling the rate of unsuccessful or guessed attempts.
- Locking accounts after no more than 10 unsuccessful attempts.

Technical controls are used to manage the quality of passwords. This will include one of the following:

- Using multi-factor authentication in conjunction with a password of at least 8 characters, with no maximum length restrictions.
- A minimum password length of at least 12 characters, with no maximum length restrictions.
- A minimum password length of at least 8 characters, with no maximum length restrictions and use automatic blocking of common passwords using a deny list

People are supported to choose unique passwords for their work accounts.

New guidance has been created on how to form passwords. It is now recommended that three random words are used to create a password that is long, difficult to guess and unique.

There is an established process to change passwords promptly if the applicant knows or suspects the password or account has been compromised.

ACCOUNT SEPARATION

Use separate accounts to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks)

THE SCOPE OF AN ORGANISATION MUST INCLUDE END-USER DEVICES

If an organisation certifies their server systems only, they ignore the threats that come from their administrators who administered those server systems. The change to this requirement closes the loop-hole where organisations were able to certify their company without including any end user devices. Cyber Essentials must now include end point devices.

ALL HIGH AND CRITICAL UPDATES MUST BE APPLIED WITHIN 14 DAYS AND REMOVE UNSUPPORTED SOFTWARE

All software on in scope devices must be:

- Licensed and supported
- Removed from devices when it becomes un-supported or removed from scope by using a defined 'sub-set' that prevents all traffic to/from the internet.
- Have automatic updates enabled where possible
- Updated, including applying any manual configuration changes required to make the update effective, within 14 days of an update being released, where:
  – The update fixes vulnerabilities described by the vendor as 'critical' or 'high risk'
  – The update addresses vulnerabilities with a CVSS v3 score of 7 or above
  – There are no details of the level of vulnerabilities the update fixes provide by the vendor

GUIDANCE ON BACKING UP

Backing up your data is not a technical requirement of Cyber Essentials, however there is now guidance on backing up important data and implementing an appropriate backup solution is highly recommended.

TWO ADDITIONAL TESTS HAVE BEEN ADDED TO THE CYBER ESSENTIALS PLUS AUDIT

1. Test to confirm account separation between user and administration accounts
2. Test to confirm MFA is required for access to cloud services.

HOW THE CHANGES WILL WORK

There will be a grace period of one year to allow organisations to make the changes for the following requirements:

1. **MFA FOR CLOUD SERVICES**
   a. The requirement will apply for administrator accounts from January 2022
   b. The MFA for users requirement will be marked for compliance from January 2023
2. **THIN CLIENTS**
   a. Thin Clients need to be supported and receiving security updates, the requirement will be marked for compliance from January 2023
   b. The new question will be for information only for first 12 months.

December 2021

3. SECURITY UPDATE MANAGEMENT

a. Unsupported software removed from scope will be marked for compliance from January 2023
b. The new question will be for **information only** for first 12 months.
c. If your organisation registers and pays for Cyber Essentials certification before 24th January 2022, you will be assessed on the old Cyber Essentials question set and have up to six months to complete your self-assessment.

The Cyber Essentials Readiness Tool will be updated with the new requirements for the 5 technical controls on 24th January 2022. If you would like to use the tool for guidance on the old question set, please access the guidance before 24th January 2022.