National Cyber Security Centre
a part of GCHQ

CYBER ESSENTIALS

Cyber Essentials: Requirements for IT Infrastructure v3.2

Cyber Essentials: Requirements for IT infrastructure v3.2

Contents

What's new in this version

- Passwordless guidance added to User Access Control
- Software definition updated
- Vulnerability fix definition added
- Passwordless definition and description added
- Update to security update management control to include vulnerabilities that are fixed by manual configuration only
- References to 'home working' changed to 'home and remote working'

A. Introducing the technical controls

We have organised the requirements under five technical controls:

1. Firewalls
2. Secure configuration
3. Security update management
4. User access control
5. Malware protection

As a Cyber Essentials scheme applicant organisation, it's your responsibility to make sure that your organisation meets all the requirements. You might also be required to supply evidence before your Certification Body can award certification at the level for which you're applying.

What you should do first:

- Establish the **boundary of scope** for your organisation, and then **determine what is in scope within this boundary**.
- Review each of the **five technical control themes** and the **controls they embody as requirements**.
- Take the necessary steps to **ensure that your organisation meets every requirement** it needs for the scope you have determined.

B. Definitions

- **Software** includes operating systems, commercial off-the-shelf applications, extensions, interpreters, scripts, libraries, network software and firewall and router firmware.
- **Devices** includes all types of hosts, networking equipment, servers, networks, and end user devices such as desktop computers, laptop computers, thin clients, tablets and smartphones — whether physical or virtual.
- **Applicant** refers to your organisation which is seeking certification, or sometimes the individual who is acting as the main point of contact, depending on context.
- A **corporate VPN** is a virtual private network that connects back to your office location, or to a virtual or cloud firewall. You must administer the VPN so you can apply the firewall controls.
- **Organisational data** includes any electronic data belonging to your organisation, for example, emails, documents, database data, financial data.
- **Organisational service** includes any software applications, cloud applications, cloud services, user interactive desktops and mobile device management (MDM) solutions that your organisation owns or subscribes to. For example: web applications, Microsoft 365, Google Workspace, mobile device management containers, Citrix Desktop, Virtual Desktop solutions or IP telephony.
- A **sub-set** is part of the organisation whose network is segregated from the rest of the organisation by a firewall or VLAN.
- **Servers** are devices that provide organisational data or services to other devices as part of your organisation's business.
- **Vulnerability fixes** include patches, updates, registry fixes, configuration changes, scripts or any other mechanism approved by the vendor to fix a known vulnerability.
- **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 vulnerability fixes. The vendor must provide the future date when they will stop providing these. (Note that the vendor doesn't need to have created the software originally, but they must be able to now modify the original software to create fixes).

- **Passwordless authentication** is an authentication method that uses a factor other than user knowledge to establish identity. Examples include but are not limited to; biometric data, physical devices, one-time codes, QR codes, and push notifications.

C. Scope

Scope overview

Your assessment and certification should cover the whole of the IT infrastructure used to carry out your organisation's business, or if necessary, a well-defined and separately managed sub-set. Either way, you must clearly define the scope boundary, namely: the business unit managing it, the network boundary and physical location. You must agree the scope with the Certification Body before assessment begins.

A sub-set can be used to define what is **in scope** or what is **out of scope** for your Cyber Essentials certification.

Please note: Organisations that choose a scope which includes their whole IT infrastructure achieve the best protection and maximise their customers' confidence.

The requirements apply to all devices and software in scope and which meet any of these conditions:

- can accept incoming network connections from untrusted internet-connected hosts
- can establish user-initiated outbound connections to devices via the internet
- control the flow of data between any of the above devices and the internet

A scope that doesn't include end user devices isn't acceptable.

Asset management and Cyber Essentials

Asset management isn't a specific Cyber Essentials control, but effective asset management can help meet all five controls, so it should be considered as a core security function.

Most business operations depend on some aspect of asset management, and cyber security shouldn't be considered in isolation, or as the primary consumer of asset information. These functions include IT operations, financial accounting, managing software licences, procurement and logistics. They may not all need the same information, but there will be overlaps and dependencies between the respective requirements. Integrating and coordinating asset management across your organisation will help reduce or manage any conflicts between these functions.

Effective asset management doesn't mean making lists or databases that are never used. It means creating, establishing and maintaining authoritative and accurate information about your assets that enables both day-to-day operations and efficient decision making when you need it. In particular, it will help you track and control devices as they're introduced into your business.

The NCSC has comprehensive guidance for organisations on asset management.

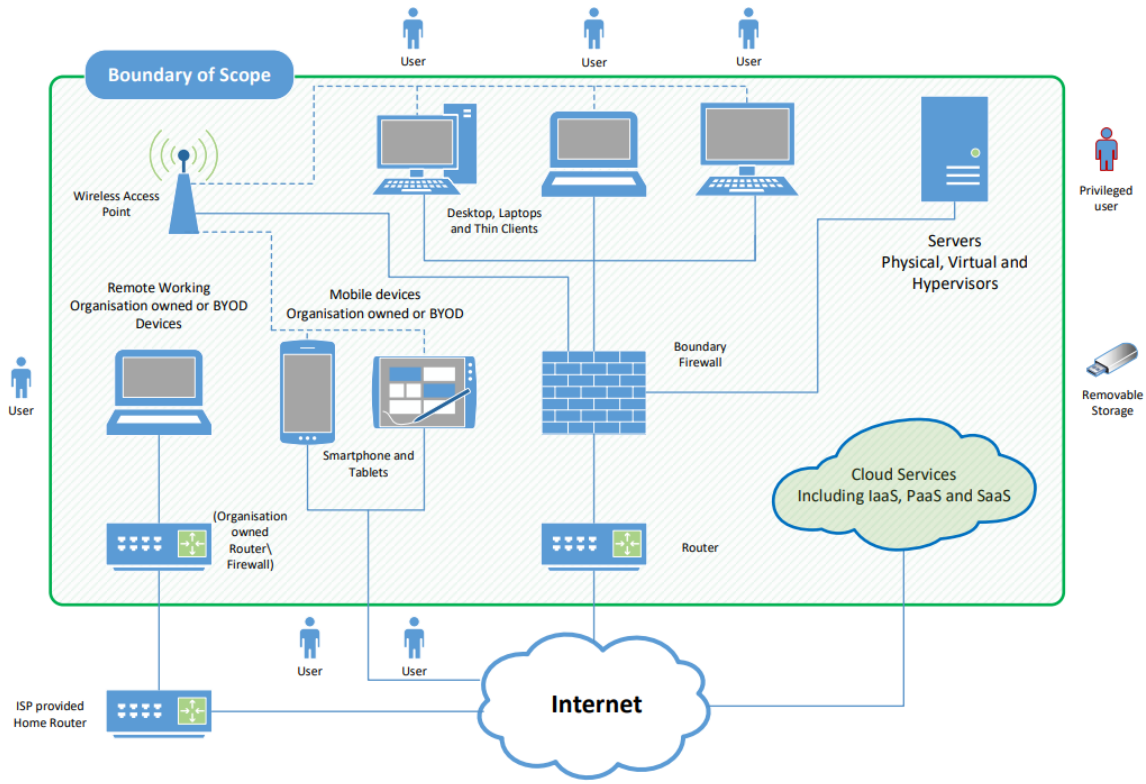

Figure 1: Scope of the requirements for IT infrastructure

i. Bring your own device (BYOD)

In addition to mobile or remote devices owned by the organisation, user-owned devices which access organisational data or services (as defined above) are **in scope**. However, all mobile or remote devices used **only** for the purpose of:

- native voice applications
- native text applications
- multi-factor authentication (MFA) applications

are **out of scope**.

Traditionally, user devices were managed centrally, which ensured consistency across the organisation. Certifying security controls in this way is more straightforward as there is a standard build or reference.

BYOD complicates matters, as users are given more freedom to 'customise' their experience making consistent implementation of the controls more challenging. Using the organisational data and services definitions to enforce strong access policies should remove some of this ambiguity.

For further information and advice on the use of BYOD please see the NCSC's guidance.

ii. Home and remote working

Our default approach is that all corporate or BYOD home/remote working devices used for your organisation's business are in scope for Cyber Essentials.

If your organisation gives the home/remote worker a router, that router is then also in scope.

All other routers are **out of scope** which means you need to apply Cyber Essentials firewall controls (such as a software firewall) on users' devices. If the home/remote worker is using a corporate VPN, their internet boundary is on the company firewall or virtual/cloud firewall.

iii. Wireless devices

Wireless devices (including wireless access points) are:

- **in scope** if they can communicate with other devices via the internet
- **out of scope** if it's not possible for an attacker to attack directly via the internet (the Cyber Essentials scheme isn't concerned with attacks that can only be launched within the signal range of the wireless device)
- **out of scope** if they are part of an ISP router at the home or remote location

iv. Cloud services

If your organisation's data or services are hosted on cloud services, these services must be **in scope**.

For cloud services, **the applicant organisation is always responsible** for ensuring all controls are implemented, but some of the controls can be implemented by the cloud service provider. Who implements which control depends on the type of cloud service. We consider three different types of cloud service:

- **Infrastructure as a Service (IaaS)** – the cloud provider delivers virtual servers and network equipment that, much like physical equipment, your organisation configures and manages. Examples of IaaS include Rackspace, Google Compute Engine, or Amazon EC2.
- **Platform as a Service (PaaS)** – the cloud provider delivers and manages the underlying infrastructure, and your organisation provides and manages the applications. Examples of PaaS include Azure Web Apps and Amazon Web Services Lambda.
- **Software as a Service (SaaS)** – the cloud provider delivers applications, and your organisation then configures the services. You must still make sure that the service is configured securely. Examples of SaaS include Microsoft 365, Dropbox and Gmail.

Who implements the controls will vary, depending how the cloud service is designed. Table 1 explains who might typically be expected to implement each control:

Requirement	IaaS	PaaS	SaaS
Firewalls	Both your organisation and the cloud provider	The cloud provider and sometimes also your organisation	The cloud provider
Secure configuration	Both your organisation and the cloud provider	Both your organisation and the cloud provider	Both your organisation and the cloud provider
Security update management	Both your organisation and the cloud provider	Both your organisation and the cloud provider	The cloud provider
User access control	Your organisation	Your organisation	Your organisation
Malware protection	Both your organisation and the cloud provider	The cloud provider and sometimes also your organisation	The cloud provider

Table 1: Explanation of who may typically implement each control

In cases where the cloud provider implements one of the controls on your behalf, you must make sure that the cloud provider has committed to implementing this via contractual clauses or documents referenced by contract, such as security statements or privacy statements. Cloud providers will often explain how they implement security in documents published in their trust centres, referencing a 'shared responsibility model.'

v. Accounts used by third parties and managed infrastructure

All accounts your organisation owns are in scope, even when those accounts are used by a third party, such as a supplier, contractor or Managed Service Provider (MSP) to manage or support your infrastructure.

If you're using externally managed services (such as remote administration), you must be able to confirm that the Cyber Essentials technical controls are being met, and be able to demonstrate this in your assessment answers.

vi. Devices used by third parties

All end user devices your organisation owns that are loaned to a third party must be included in the assessment scope.

For devices not owned by your organisation, Table 2 explains what is in and out of scope:

	Owned by your organisation	**Owned by a third party**	**BYOD**
Employee	✓	N/A	✓
Volunteer	✓	N/A	✓
Trustee	✓	N/A	✓
University research assistant	✓	N/A	✓
Student	✓	N/A	✘
MSP administrator	✓	✘	✘
Third party contractor	✓	✘	✘
Customer	✓	✘	✘

Table 2: what is in and out of scope for devices not owned by your organisation

Key: ✓ in scope ✘ out of scope

For devices out of scope of the assessment, your organisation is still responsible for confirming that the devices interacting with organisational services and data are configured correctly. It's up to you how to achieve this, as it falls outside of the assessment scope.

vii. Web applications

Publicly available commercial web applications (rather than apps developed in-house) are in scope by default. Bespoke and custom

components of web applications are out of scope. The best way to mitigate vulnerabilities in applications is robust development and testing in line with commercial best practice, such as the OWASP Application Security Verification Standard | OWASP Foundation.

D. Requirements by technical control theme

1. Firewalls

Applies to: boundary firewalls, desktop computers, laptops, routers, servers, IaaS, PaaS, SaaS.

Aim

To make sure that only secure and necessary network services can be accessed from the internet.

Introduction

All devices run network services to allow them to communicate with other devices and services. By restricting access to these services, you reduce your exposure to attacks. You can do this using firewalls or network devices with firewall functionality. For cloud services, you can achieve this using data flow policies.

A boundary firewall is a network device which can restrict the inbound and outbound network traffic to services on its network of computers and mobile devices. It can help protect against cyber attacks by implementing restrictions, known as 'firewall rules,' which can allow or block traffic depending on its source, destination and type of communication protocol.

Alternatively, if your organisation doesn't control the network to which a device connects, you must configure a software firewall on the device. This works in the same way as a boundary firewall but only protects the single device on which it's configured. This approach allows for more tailored rules and means that the rules apply to the device wherever it's used. But you should note that this creates a greater administrative overhead when managing firewall rules.

Requirements

You must protect every device in scope with a correctly configured firewall (or network device with firewall functionality).

Information: Most desktop and laptop operating systems now come with a software firewall pre-installed, we advise that these are turned on in preference to a third-party firewall application.

For all firewalls (or network devices with firewall functionality), your organisation must:

- change default administrative passwords to a strong and unique password (see password-based authentication) – or disable remote administrative access entirely
- prevent access to the administrative interface (used to manage firewall configuration) from the internet, unless there is a clear and documented business need, and the interface is protected by one of the following controls:
    - multi-factor authentication (see MFA details below)
    - an IP allow list that limits access to a small range of trusted addresses combined with a properly managed password authentication approach
- block unauthenticated inbound connections by default
- ensure inbound firewall rules are approved and documented by an authorised person, and include the business need in the documentation
- remove or disable unnecessary firewall rules, when they are no longer needed

Make sure you use a software firewall on devices which are used on untrusted networks, such as public wifi hotspots.

2. Secure configuration

Applies to: servers, desktop computers, laptops, tablets, mobile phones, thin clients, IaaS, PaaS, SaaS.

Aim

Ensure that computers and network devices are properly configured to:

- reduce vulnerabilities
- provide only the services required to fulfil their role

Introduction

The default configurations of computers and network devices aren't always secure. Standard out-of-the-box configurations often include one or more weak points such as:

- an administrative account with a pre-set, publicly known default password or without multi-factor authentication enabled
- pre-enabled but unnecessary user accounts (sometimes with special access privileges)
- pre-installed but unnecessary applications or services

These default installations can allow attackers to gain unauthorised access to your organisation's sensitive information.

But by applying some simple technical controls when installing computers and network devices, you can minimise vulnerabilities and protect against common types of attack.

Requirements

Computers and network devices

Your organisation must proactively manage your computers and network devices. You must regularly:

- remove and disable unnecessary user accounts (such as guest accounts and administrative accounts that won't be used)

- change any default or guessable account passwords (see password-based authentication)
- remove or disable unnecessary software (including applications, system utilities and network services)
- disable any auto-run feature which allows file execution without user authorisation (such as when they are downloaded)
- ensure users are authenticated before allowing them access to organisational data or services
- ensure appropriate device locking controls (see 'device unlocking', below) for users that are physically present

Device unlocking credentials

If a device requires a user's physical presence to access a device's services (such as logging on to a laptop or unlocking a mobile phone), a credential such as a biometric, password or PIN must be in place before a user can gain access to the services.

You must protect your chosen authentication method (which can be biometric authentication, password or PIN) against brute-force attacks. When it's possible to configure, you should apply one of the following:

- 'throttling' the rate of attempts, so that the length of time the user must wait between attempts increases with each unsuccessful attempt. You shouldn't allow more than 10 guesses in 5 minutes
- locking devices after more than 10 unsuccessful attempts.

When the vendor doesn't allow you to configure the above, use the vendor's default setting.

Technical controls must be used to manage the quality of credentials. If credentials are just to unlock a device, use a minimum password or PIN length of at least 6 characters. When the device unlocking credentials are also used for authentication, you must apply the full password requirements to the credentials described in 'user access controls.'

3. Security update management

Applies to: servers, desktop computers, laptops, tablets, mobile phones, firewalls, routers, IaaS, PaaS, SaaS.

Aim

Ensure that devices and software are not vulnerable to known security issues for which fixes are available.

Introduction

Any device that runs software can contain security flaws, known as vulnerabilities.

Vulnerabilities are regularly discovered in all sorts of software. Once discovered, malicious individuals or groups move quickly to misuse (or 'exploit') vulnerabilities to attack computers and networks.

Product vendors provide fixes for vulnerabilities identified in products that they still support, in the form of patches, security updates, registry fixes, scripts, configuration changes or any other mechanism prescribed by the vendor to fix a known vulnerability. These may be made available to customers immediately or on a regular release schedule (perhaps monthly).

Requirements

You must make sure that all software in scope is kept up to date. All software on in-scope devices must:

- be licensed and supported
- removed from devices when it becomes unsupported or removed from scope by using a defined sub-set that prevents all traffic to / from the internet
- have automatic updates enabled where possible
- be updated, including vulnerability fixes, within 14 days* of release, where:

- the update fixes vulnerabilities described by the vendor as ‘critical’ or ‘high risk’
- the update addresses vulnerabilities with a CVSS v3 base score of 7 or above
- there are no details of the level of vulnerabilities the update fixes provided by the vendor

Please note: For optimum security we strongly recommend (but it’s not mandatory) that all released updates are applied within 14 days of release.

***It's important that updates are applied as soon as possible. 14 days is considered a reasonable period to be able to implement this requirement. Any longer would constitute a serious security risk while a shorter period may not be practical.

Information: If the vendor uses different terms to describe the severity of vulnerabilities, see the precise definition in the Common Vulnerability Scoring System (CVSS). For the purposes of the Cyber Essentials scheme, ‘critical’ or ‘high risk’ vulnerabilities are those with a CVSS v3 base score of 7 or above or are identified by the vendor as 'critical or high risk'.

Caution: Some vendors release security updates for multiple issues with differing severity levels as a single update. If such an update covers any ‘critical’ or ‘high risk’ issues then it must be installed within 14 days.

4. User access control

Applies to: servers, desktop computers, laptops, tablets, mobile phones, IaaS, PaaS, SaaS.

Aim

Ensure that user accounts:

- are assigned to authorised individuals only
- provide access to only those applications, computers and networks the user needs to carry out their role

Introduction

Every active user account in your organisation facilitates access to devices and applications, and to sensitive business information. By making sure that only authorised individuals have user accounts, and that they're only granted as much access as they need to carry out their role, you reduce the risk of information being stolen or damaged.

Compared to normal user accounts, accounts with special access privileges have enhanced access to devices, applications and information. If these accounts are compromised, an attacker could take advantage of their greater accesses to corrupt information on a large scale, disrupt business processes or gain unauthorised access to other devices in the organisation.

Administrative accounts are especially highly privileged, for example. These accounts typically allow the user to:

- execute software that can make significant and security-related changes to the operating system
- make changes to the operating system for some or all users
- create new accounts and allocate privileges

All types of administrators will have this kind of account, including domain administrators and local administrators.

This is important because if a user opens a malicious URL or email attachment, the malware would typically be executed with the same privilege level of the user's account. This is why it's important to take special care allocating and using privileged accounts.

Example: Jody is logged in with an administrative account. If Jody opens a malicious URL or email attachment, any associated malware is likely to acquire administrative privileges. Unfortunately, this is exactly what happens. Using Jody's administrative privileges, a type of malware known as ransomware encrypts all of the data on the network and then demands a ransom. The ransomware was able to encrypt far more data than would have been possible with standard user privileges, making the problem that much more serious.

Requirements

Your organisation must be in control of your user accounts and the access privileges that allow access to your organisational data and services. It's important to note that this also includes third party accounts – for example accounts used by your support services. You also need to understand how user accounts authenticate and manage the authentication accordingly.

This means your organisation must:

- have in place a process to create and approve user accounts
- authenticate users with unique credentials before granting access to applications or devices (see password-based authentication)
- remove or disable user accounts when they're no longer required (for example, when a user leaves the organisation or after a defined period of account inactivity)
- implement MFA, where available – authentication to cloud services must always use MFA
- 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)
- remove or disable special access privileges when no longer required (when a member of staff changes role, for example)

Password-based authentication

All user accounts require the user to authenticate.

Where this is carried out using a password, you should put in place the following protective measures:

- Passwords are protected against brute-force password guessing by implementing at least one of:
    - multi-factor authentication (see below)
    - 'throttling' the rate of attempts, so that the length of time the user must wait between attempts increases with each unsuccessful attempt – you shouldn't allow more than 10 guesses in 5 minutes
    - locking devices after no more than 10 unsuccessful attempts

- Use technical controls to manage the quality of passwords. This will include one of the following:
    - Using multi-factor authentication (see below)
    - 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.

- Support users to choose unique passwords for their work accounts by:
    - educating people about avoiding common passwords, such as a pet's name, common keyboard patterns or passwords they have used elsewhere. This could include teaching people to use the password generator feature built into some password managers.
    - encouraging people to choose longer passwords by promoting the use of multiple words (a minimum of three) to create a password (such as the NCSC's guidance on using three random words)
    - providing usable secure storage for passwords (for example a password manager or secure locked cabinet) with clear information about how and when it can be used.

- not enforcing regular password expiry
- not enforcing password complexity requirements

You should also make sure there is an established process in place to change passwords promptly if you know or suspect a password or account has been compromised.

Multi-factor authentication (MFA)

As well as providing an extra layer of security for passwords that aren't protected by the other technical controls, you should always use multi-factor authentication to give administrative accounts extra security, and accounts that are accessible from the internet.

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

There are four types of additional factor to consider:

- a managed/enterprise device
- an app on a trusted device
- a physically separate token
- a known or trusted account

Additional factors should be chosen so that they are usable and accessible. You might need to carry out user testing to decide what is best for your users. For more information see the NCSC's guidance on MFA.

Information: SMS is not the most secure type of MFA, but still offers a huge advantage over not using any MFA at all. Any multi-factor authentication is better than not having it at all. However, if there are alternatives available that will work for your situation, we recommend you use these instead of SMS.

Passwordless authentication

Passwordless authentication is a method of verifying identity without using traditional passwords.

Common examples of passwordless authentication include:

- **Biometric authentication**: Uses biological traits of the user such as fingerprints or facial features to confirm their identity.
- **Security keys or tokens**: Physical hardware devices such as USB security keys or smart cards.
- **One-time codes**: Temporary codes are sent via email, SMS, or a mobile app.
- **Push notifications**: A prompt on a smartphone to approve or deny a login attempt.

This helps to avoid many of the problems with traditional passwords which can be forgotten, stolen, or brute-forced.

5. Malware protection

Applies to: servers, desktop computers, laptops, tablets, mobile phones, IaaS, PaaS, SaaS.

Aim

To restrict execution of known malware and untrusted software, from causing damage or accessing data.

Introduction

Malware, such as computer viruses, worms and ransomware, is software that has been written and distributed deliberately to perform malicious actions. Potential sources include; malicious email attachments, downloads (including those from application stores), and direct installation of unauthorised software.

If a system is infected, your organisation is likely to suffer from problems like malfunctioning systems, data loss, or onward infection that goes unseen until it causes harm elsewhere.

You can largely avoid the potential for harm by:

- preventing malware from being delivered to devices
- preventing malware from running on devices

Example: Acme Corporation implements code signing alongside a rule that allows only vetted applications from the device application store to execute on devices. Unsigned and unapproved applications will not run on devices. The fact that users can only install trusted (allow-listed) applications leads to a reduced risk of malware infection.

Requirements

You must make sure that a malware protection mechanism is active on all devices in scope. For each device, you must use at least one of the options listed below. In most modern products these options are built into the software supplied. Alternatively, you can purchase products from a third-

party provider. In all cases the software must be active, kept up to date in accordance with the vendors instructions, and configured to work as detailed below:

Anti-malware software (option for in scope devices running Windows or MacOS including servers, desktop computers, laptop computers)

If you use anti-malware software to protect your device it must be configured to:

- be updated in line with vendor recommendations
- prevent malware from running
- prevent the execution of malicious code
- prevent connections to malicious websites over the internet.

Application allow listing (option for all in scope devices)

Only approved applications, restricted by code signing, are allowed to execute on devices. You must:

- actively approve such applications before deploying them to devices
- maintain a current list of approved applications, users must not be able to install any application that is unsigned or has an invalid signature.

E. Further guidance

Backing up your data

Backing up means creating a copy of your information and saving it to another device or to cloud storage (online).

Backing up regularly means you will always have a recent version of your information saved. This will help you recover quicker if your data is lost or stolen.

You can also turn on automatic backup. This will regularly save your information into cloud storage, without you having to remember.

If you back up your information to a USB stick or an external hard drive, disconnect it from your computer when a backup isn't being done.

Backing up your data is not a technical requirement of Cyber Essentials; however we highly recommend implementing an appropriate backup solution.

Zero trust and Cyber Essentials

Network architecture is changing. More services are moving to the cloud and use of Software as a Service (SaaS) continues to grow.

At the same time, many organisations are embracing flexible working, which means lots of different device types may connect to your systems from many locations. It's also increasingly common for organisations to share data with their partners and guest users, which requires more granular access control policies.

Zero trust architecture is designed to cope with these changing conditions by enabling an improved user experience for remote access and data sharing.

A zero trust architecture is an approach to system design where inherent trust in the network is removed. Instead, the network is assumed hostile and each access request is verified, based on an access policy. Confidence in a request is achieved by building context, which relies on strong authentication, authorisation, device health, and value of the data being accessed.

As organisations move towards zero trust architecture models, we have considered it in this context, and are confident that implementing the technical controls doesn't prevent you using a zero trust architecture as defined by the NCSC guidance.