YourIT!
Your Logo Goes Here

Cyber Essentials

Policies and Procedures

Prepared for: Client Company

Prepared by: YourIT Company

Table of Contents

46	UK Cyber Essentials Malware Protection-1.1.4 - Anti-Malware Protection - Malicious Website Connections
47	UK Cyber Essentials Malware Protection-1.2 - Application Whitelisting - Allow Listing
48	UK Cyber Essentials Malware Protection-1.2.1 - Application Whitelisting - Allow Listing - Prior Approval
49	UK Cyber Essentials Malware Protection-1.2.2 - Application Whitelisting - Allow Listing - Maintain List
50	UK Cyber Essentials Malware Protection-1.3 - Sandboxing
51	UK Cyber Essentials Malware Protection-1.3.1 - Sandboxing - Applications
52	UK Cyber Essentials Malware Protection-1.3.2 - Sandboxing - Data Stores
53	UK Cyber Essentials Malware Protection-1.3.3 - Sandboxing - Peripherals
54	UK Cyber Essentials Malware Protection-1.3.4 - Sandboxing - Network Access
55	UK Cyber Essentials Security Update Management-1 - Security Update Management
56	UK Cyber Essentials Security Update Management-1.1 - Security Update Management - Licensed Software
57	UK Cyber Essentials Security Update Management-1.2 - Security Update Management - Unsupported Software
58	UK Cyber Essentials Security Update Management-1.3 - Security Update Management - Automatic Updates
59	UK Cyber Essentials Security Update Management-1.4 - Security Update Management - Critical Updates
60	UK Cyber Essentials Data Backup-1 - Data Backup - Recommended

Purpose

Software includes operating systems, commercial off-the-shelf applications, plugins, interpreters, scripts, libraries, network software and 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 mobile phones (smartphones) — whether physical or virtual.

• Applicant means the organisation seeking certification, or sometimes the individual acting as the main point of contact, depending on context.

• A corporate VPN is a Virtual Private Network solution that connects back to the applicant's office location or to a virtual/cloud firewall. This must be administered by the applicant organisation so that the firewall controls can be applied.

• Organisational data includes any electronic data belonging to the applicant organisation. For example emails, office documents, database data, financial data.

• Organisational service includes any software applications, Cloud applications, Cloud services, User Interactive desktops and Mobile Device management solutions owned or subscribed to by the applicant organisation. For example: Web applications, Microsoft Office 365, Google Workspace, Mobile Device Management Containers, Citrix Desktop, Virtual Desktop solutions, IP Telephony.

• 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.

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

• 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 updates or patches. 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.

Scope

Assessment and certification should cover the whole of the IT infrastructure used to perform the business of the Applicant, or if necessary, a well-defined and separately managed sub-set. Either way, the boundary of the scope must be clearly defined in terms of the business unit managing it, the network boundary and physical location. The scope must be agreed between the Applicant and 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 Cyber Essentials.

Information: Organisations that choose a scope that includes the whole IT infrastructure achieve the best protection and increase customer confidence.

The requirements apply to all the devices and software that are within the boundary of the scope and that meet the any of these conditions:

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

A scope that does not include end-user devices is not acceptable.

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 applications

are out of scope.

Traditionally, user devices were managed through centralised administration, ensuring consistency across the organisation. In such cases, certification of the security controls is straightforward as there will be a standard build or reference to assess.

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.

Home working
The default approach is that all corporate or BYOD home working devices used for applicant business purposes within the home location are in scope for Cyber Essentials.

Internet Service Provider (ISP) routers and user provided routers are out of scope which means that the Cyber Essentials firewall controls need to be applied on the user devices (e.g. a software firewall).

If a router is supplied to the home worker by the applicant organisation, then that router will be in scope.

If the home worker is using a corporate VPN, their internet boundary is on the company firewall or virtual/cloud firewall.

Wireless devices
Wireless devices (including wireless access points) are:

- in scope if they can communicate with other devices via the Internet

- not in scope if it is not possible for an attacker to attack directly from the Internet (the Cyber Essentials scheme is not concerned with attacks that can only be launched from within the signal range of the wireless device)

- not in scope if they are part of an ISP router within the home location

Externally managed services — cloud
If the Applicant's data or services are hosted on cloud services, then these services must be in scope. In cloud services the Applicant is always responsible for ensuring all the 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 are configured and managed by the Applicant, much like physical equipment would be. 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 the Applicant 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 to the Applicant, and the Applicant configures the services. The Applicant must still take time to ensure the service is configured securely. Examples of SaaS include Microsoft 365, Dropbox, and Gmail.

Where the cloud provider implements a control, the Applicant must satisfy themselves that this has been done by the cloud provider committing to implementation within 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, which will include reference to a "shared responsibility model".

Externally managed services — other
Where the Applicant is using other externally managed services (such as remote administration) it may not be possible for the Applicant to meet all the requirements directly. The Applicant may choose whether or not to include these services within the boundary of scope, according to feasibility.

If included, then the Applicant must be able to attest that the requirements that are outside of the Applicant's control are being adequately met by the service provider. Existing evidence may be considered (such as that provided through PCI certification of a cloud service, and ISO 27001 certifications that cover an appropriate scope).

Web applications
Commercial web applications created by development companies (rather than in-house developers) and which are publicly accessible from the Internet are in scope by default. Bespoke and custom components of web applications are not in scope. The primary mitigation against vulnerabilities in such applications is robust development and testing in line with commercial best practices, such as the Open Web Application Security Project (OWASP) standards.

Sanctions/Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

UK Cyber Essentials Firewalls-1 - Properly Configured Firewall

UK Cyber Essentials - v3.0	Other Requirements
Firewalls-1 Properly Configured Firewall	N/A

Policy
Every device that is in scope must be protected by a correctly configured firewall (or equivalent network device).

Guidance
Applies to: boundary firewalls; desktop computers; laptop computers; routers; servers; IaaS; PaaS; SaaS.
Objective
Ensure that only safe and necessary network services can be accessed from the Internet.

Introduction
All devices run network services, which create some form of communication with other devices and services. By restricting access to these services, you reduce your exposure to attacks. This can be achieved using firewalls and equivalent network devices, or data flow policies in cloud services.

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 according to its source, destination and type of communication protocol.

Alternatively, where an organisation does not control the network a device is connected to, a software firewall must be configured on a device. This works in the same way as a boundary firewall but only protects the single device on which it is configured. This approach can provide for more tailored rules and means that the rules apply to the device wherever it is used. However, this increases the administrative overhead of managing firewall rules.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- UKCE-1 - Properly Configure Firewall(s): Protect all in-scope devices with a properly-configured firewall.

References
- UK National Cyber Security Centre - https://www.ncsc.gov.uk/cyberessentials/overview
- Cyber Essentials Readiness Toolkit - https://getreadyforcyberessentials.iasme.co.uk/questions/
- Cyber Essentials Certification - https://iasme.co.uk/cyber-essentials/

UK Cyber Essentials Firewalls-1.1 - Change Firewall Password or Disable Remote Administration

UK Cyber Essentials - v3.0	Other Requirements
Firewalls-1.1 Change Firewall Password or Disable Remote Administration	N/A

Policy
For all firewalls (or equivalent network devices), the organisation must routinely change any default administrative password to an alternative that is difficult to or disable remote administrative access entirely.

Guidance
Firewall configuration and management are best performed by a qualified technician certified by the firewall manufacturer.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- UKCE-2 - Change Firewall Password or Disable Remote Administration: Routinely change any default administrative password to an alternative that is difficult to break or disable remote administrative access entirely

References
- UK National Cyber Security Centre - https://www.ncsc.gov.uk/cyberessentials/overview
- Cyber Essentials Readiness Toolkit - https://getreadyforcyberessentials.iasme.co.uk/questions/
- Cyber Essentials Certification - https://iasme.co.uk/cyber-essentials/

UK Cyber Essentials Firewalls-1.2 - Prevent Internet Administrative Access

UK Cyber Essentials - v3.0	Other Requirements
Firewalls-1.2 Prevent Internet Administrative Access	N/A

Policy
For all firewalls (or equivalent network devices), the organisation must routinely 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 - an IP allow list that limits access to a small range of trusted addresses combined with a properly managed password authentication approach.

Guidance
Firewall configuration and management are best performed by a qualified technician certified by the firewall manufacturer.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- UKCE-3 - Prevent Internet Administrative Access to Firewall: Routinely 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 - an IP allow list that limits access to a small range of trusted addresses combined with a properly managed password authentication approach.

References
- UK National Cyber Security Centre - https://www.ncsc.gov.uk/cyberessentials/overview
- Cyber Essentials Readiness Toolkit - https://getreadyforcyberessentials.iasme.co.uk/questions/
- Cyber Essentials Certification - https://iasme.co.uk/cyber-essentials/

UK Cyber Essentials Firewalls-1.3 - Block Unauthenticated Inbound Connections

UK Cyber Essentials - v3.0	Other Requirements
Firewalls-1.3 Block Unauthenticated Inbound Connections	N/A

Policy
For all firewalls (or equivalent network devices), the organisation must routinely block unauthenticated inbound connections by default.

Guidance
Firewall configuration and management are best performed by a qualified technician certified by the firewall manufacturer.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- UKCE-4 - Block Unauthenticated Inbound Connections: For all firewalls (or equivalent network devices), the organisation must routinely block unauthenticated inbound connections by default.

References
- UK National Cyber Security Centre - https://www.ncsc.gov.uk/cyberessentials/overview
- Cyber Essentials Readiness Toolkit - https://getreadyforcyberessentials.iasme.co.uk/questions/
- Cyber Essentials Certification - https://iasme.co.uk/cyber-essentials/

UK Cyber Essentials Firewalls-1.4 - Approve and Document Firewall Rules

UK Cyber Essentials - v3.0	Other Requirements
Firewalls-1.4 Approve and Document Firewall Rules	N/A

Policy
For all firewalls (or equivalent network devices), the organisation must routinely ensure inbound firewall rules are approved and documented by an authorised individual;
the business need must be included in the documentation.

Guidance
Firewall configuration and management are best performed by a qualified technician certified by the firewall manufacturer.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- UKCE-5 - Approve and Document Firewall Rules: For all firewalls (or equivalent network devices), the organisation must routinely ensure inbound firewall rules are approved and documented by an authorised individual; the business need must be included in the documentation.

References
- UK National Cyber Security Centre - https://www.ncsc.gov.uk/cyberessentials/overview
- Cyber Essentials Readiness Toolkit - https://getreadyforcyberessentials.iasme.co.uk/questions/
- Cyber Essentials Certification - https://iasme.co.uk/cyber-essentials/

UK Cyber Essentials Firewalls-1.5 - Remove or Disable Unnecessary Rules

UK Cyber Essentials - v3.0	Other Requirements
Firewalls-1.5 Remove or Disable Unnecessary Rules	N/A

Policy
For all firewalls (or equivalent network devices), remove or disable unnecessary firewall rules quickly, when they are no longer needed.

Guidance
Firewall configuration and management are best performed by a qualified technician certified by the firewall manufacturer.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- UKCE-6 - Remove or Disable Unnecessary Rules: For all firewalls (or equivalent network devices), remove or disable unnecessary firewall rules quickly, when they are no longer needed.

References
- UK National Cyber Security Centre - https://www.ncsc.gov.uk/cyberessentials/overview
- Cyber Essentials Readiness Toolkit - https://getreadyforcyberessentials.iasme.co.uk/questions/
- Cyber Essentials Certification - https://iasme.co.uk/cyber-essentials/

UK Cyber Essentials Firewalls-1.6 - Software Firewall

UK Cyber Essentials - v3.0	Other Requirements
Firewalls-1.6 Software Firewall	N/A

Policy
For all firewalls (or equivalent network devices), the organisation must routinely use a software firewall on devices which are used on untrusted networks, such as public Wi-Fi hotspots.

Guidance
Firewall configuration and management are best performed by a qualified technician certified by the firewall manufacturer.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- UKCE-7 - Software Firewall: For all firewalls (or equivalent network devices), the organisation must routinely use a software firewall on devices which are used on untrusted networks, such as public Wi-Fi hotspots.

References
- UK National Cyber Security Centre - https://www.ncsc.gov.uk/cyberessentials/overview
- Cyber Essentials Readiness Toolkit - https://getreadyforcyberessentials.iasme.co.uk/questions/
- Cyber Essentials Certification - https://iasme.co.uk/cyber-essentials/

UK Cyber Essentials Secure Configuration-1 - Computers and Network Devices

UK Cyber Essentials - v3.0	Other Requirements
Secure Configuration-1 Computers and Network Devices	N/A

Policy
The organisation must be active in its management of computers and network devices.

Guidance
Applies to: servers; desktop computers; laptop computers; tablets; mobile phones; thin clients; IaaS; PaaS; SaaS

Computers and network devices are not always secure in their default configurations. Standard, out-of-the-box configurations often include one or more weak points such as:
• an administrative account with a predetermined, 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

Default installations of computers and network devices can provide cyber attackers with a variety of opportunities to gain unauthorised access to an organisation's sensitive information — often with ease.

By applying some simple technical controls when installing computers and network devices you can minimise inherent vulnerabilities and increase protection against common types of cyber attack.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- UKCE-8 - Computers and Network Devices: The organisation must be active in its management of computers and network devices.

References
- UK National Cyber Security Centre - https://www.ncsc.gov.uk/cyberessentials/overview
- Cyber Essentials Readiness Toolkit - https://getreadyforcyberessentials.iasme.co.uk/questions/
- Cyber Essentials Certification - https://iasme.co.uk/cyber-essentials/

UK Cyber Essentials Secure Configuration-1.1 - Computers and Network Devices - User Accounts

UK Cyber Essentials - v3.0	Other Requirements
Secure Configuration-1.1 Computers and Network Devices - User Accounts	N/A

Policy
The organisation must be active in its management of computers and network devices. It must routinely remove and disable unnecessary user accounts (such as guest accounts and administrative accounts that won't be used).

Guidance
Applies to: servers; desktop computers; laptop computers; tablets; mobile phones; thin clients; IaaS; PaaS; SaaS

Computers and network devices are not always secure in their default configurations. Standard, out-of-the-box configurations often include one or more weak points such as:
• an administrative account with a predetermined, 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

Default installations of computers and network devices can provide cyber attackers with a variety of opportunities to gain unauthorised access to an organisation's sensitive information — often with ease.

By applying some simple technical controls when installing computers and network devices you can minimise inherent vulnerabilities and increase protection against common types of cyber attack.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- UKCE-9 - Computers and Network Devices - User Accounts: Remove and disable unnecessary user accounts (such as guest accounts and administrative accounts that won't be used).

References
- UK National Cyber Security Centre - https://www.ncsc.gov.uk/cyberessentials/overview
- Cyber Essentials Readiness Toolkit - https://getreadyforcyberessentials.iasme.co.uk/questions/
- Cyber Essentials Certification - https://iasme.co.uk/cyber-essentials/

UK Cyber Essentials Secure Configuration-1.2 - Computers and Network Devices -Passwords

UK Cyber Essentials - v3.0	Other Requirements
Secure Configuration-1.2 Computers and Network Devices -Passwords	N/A

Policy
The organisation must be active in its management of computers and network devices. It must routinely change any default or guessable account passwords (see password-based authentication).

Guidance
Applies to: servers; desktop computers; laptop computers; tablets; mobile phones; thin clients; IaaS; PaaS; SaaS

Computers and network devices are not always secure in their default configurations. Standard, out-of-the-box configurations often include one or more weak points such as:
• an administrative account with a predetermined, 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

Default installations of computers and network devices can provide cyber attackers with a variety of opportunities to gain unauthorised access to an organisation's sensitive information — often with ease.

By applying some simple technical controls when installing computers and network devices you can minimise inherent vulnerabilities and increase protection against common types of cyber attack.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- UKCE-10 - Computers and Network Devices -Passwords: Change any default or guessable account passwords (see password-based authentication).

References
- UK National Cyber Security Centre - https://www.ncsc.gov.uk/cyberessentials/overview
- Cyber Essentials Readiness Toolkit - https://getreadyforcyberessentials.iasme.co.uk/questions/
- Cyber Essentials Certification - https://iasme.co.uk/cyber-essentials/

UK Cyber Essentials Secure Configuration-1.3 - Computers and Network Devices - Unnecessary Software

UK Cyber Essentials - v3.0	Other Requirements
Secure Configuration-1.3 Computers and Network Devices - Unnecessary Software	N/A

Policy
The organisation must be active in its management of computers and network devices. It must routinely remove or disable unnecessary software (including applications, system utilities and network services).

Guidance
Applies to: servers; desktop computers; laptop computers; tablets; mobile phones; thin clients; IaaS; PaaS; SaaS

Computers and network devices are not always secure in their default configurations. Standard, out-of-the-box configurations often include one or more weak points such as:
• an administrative account with a predetermined, 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

Default installations of computers and network devices can provide cyber attackers with a variety of opportunities to gain unauthorised access to an organisation's sensitive information — often with ease.

By applying some simple technical controls when installing computers and network devices you can minimise inherent vulnerabilities and increase protection against common types of cyber attack.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- UKCE-11 - Computers and Network Devices - Unnecessary Software: Remove or disable unnecessary software (including applications, system utilities and network services).

References
- UK National Cyber Security Centre - https://www.ncsc.gov.uk/cyberessentials/overview
- Cyber Essentials Readiness Toolkit - https://getreadyforcyberessentials.iasme.co.uk/questions/
- Cyber Essentials Certification - https://iasme.co.uk/cyber-essentials/

UK Cyber Essentials Secure Configuration-1.4 - Computers and Network Devices - Auto-run Features

UK Cyber Essentials - v3.0	Other Requirements
Secure Configuration-1.4 Computers and Network Devices - Auto-run Features	N/A

Policy
The organisation must be active in its management of computers and network devices. It must routinely disable any auto-run feature which allows file execution without user authorisation (such as when they are downloaded from the Internet).

Guidance
Applies to: servers; desktop computers; laptop computers; tablets; mobile phones; thin clients; IaaS; PaaS; SaaS

Computers and network devices are not always secure in their default configurations. Standard, out-of-the-box configurations often include one or more weak points such as:
• an administrative account with a predetermined, 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

Default installations of computers and network devices can provide cyber attackers with a variety of opportunities to gain unauthorised access to an organisation's sensitive information — often with ease.

By applying some simple technical controls when installing computers and network devices you can minimise inherent vulnerabilities and increase protection against common types of cyber attack.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- UKCE-12 - Computers and Network Devices - Auto-run Features: Disable any auto-run feature which allows file execution without user authorisation (such as when they are downloaded from the Internet).

References
- UK National Cyber Security Centre - https://www.ncsc.gov.uk/cyberessentials/overview
- Cyber Essentials Readiness Toolkit - https://getreadyforcyberessentials.iasme.co.uk/questions/
- Cyber Essentials Certification - https://iasme.co.uk/cyber-essentials/

Truncated Sample Report