YourIT!
Your Logo Goes Here

Cyber Essentials

Policies and Procedures

Prepared for: Client Company

Prepared by: YourIT Company

YourIT!
Your Logo Goes Here

Table of Contents

01	Purpose
02	Scope
03	Sanctions/Compliance
04	Data Backup-1 - Data Backup - Recommended
05	Device Unlocking Credentials-1 - Device Unlocking Credentials
06	Device Unlocking Credentials-1.1 - Device Unlocking Credentials - Brute Force Attack Prevention
07	Device Unlocking Credentials-1.2 - Device Unlocking Credentials - Technical Controls
08	Firewalls-1 - Properly Configured Firewall
09	Firewalls-1.1 - Change Firewall Password or Disable Remote Administration
10	Firewalls-1.2 - Prevent Internet Administrative Access
11	Firewalls-1.3 - Block Unauthenticated Inbound Connections
12	Firewalls-1.4 - Approve and Document Firewall Rules
13	Firewalls-1.5 - Remove or Disable Unnecessary Rules
14	Firewalls-1.6 - Software Firewall
15	Malware Protection-1 - Malware Protection
16	Malware Protection-1.1 - Anti-Malware Protection
17	Malware Protection-1.1.1 - Anti-Malware Protection - Active on all Devices in Scope
18	Malware Protection-1.1.2 - Anti-Malware Protection - Updates
19	Malware Protection-1.1.3 - Anti-Malware Protection - Prevent Execution of Malicious Code
20	Malware Protection-1.1.4 - Anti-Malware Protection - Malicious Website Connections
21	Malware Protection-1.2 - Application Whitelisting - Allow Listing - Prior Approval
22	Malware Protection-1.2.1 - Application Whitelisting - Allow Listing - Maintain List
23	Multi-Factor Authentication (MFA)-1 - Multi-Factor Authentication (MFA)
24	Multi-Factor Authentication (MFA)-1.1 - Multi-Factor Authentication (MFA) - Password Length
25	Multi-Factor Authentication (MFA)-1.2 - Multi-Factor Authentication (MFA) - Types
26	Password-based Authentication-1 - Password-based authentication
27	Password-based Authentication-1.1 - Password-based authentication

	- Brute-force Protection
28	Password-based Authentication-1.2 - Password-based authentication - Password Technical Controls
29	Password-based Authentication-1.3 - Password-based authentication - Unique Passwords
30	Password-based Authentication-1.3.1 - Password-based authentication - User Training
31	Password-based Authentication-1.3.2 - Password-based authentication - Long Passwords
32	Password-based Authentication-1.3.3 - Password-based authentication - Password Storage/Password Manager
33	Password-based Authentication-1.3.4 - Password-based authentication - Password Expiry
34	Password-based Authentication-1.3.5 - Password-based authentication - Password Complexity Requirements
35	Password-based Authentication-1.4 - Password-based authentication - Immediate Password Change
36	Passwordless Authentication-1 - Passwordless Authentication - Types
37	Secure Configuration-1 - Computers and Network Devices
38	Secure Configuration-1.1 - Computers and Network Devices - User Accounts
39	Secure Configuration-1.2 - Computers and Network Devices - Passwords
40	Secure Configuration-1.3 - Computers and Network Devices - Unnecessary Software
41	Secure Configuration-1.4 - Computers and Network Devices - Auto-run Features
42	Secure Configuration-1.5 - Computers and Network Devices - User Authentication
43	Secure Configuration-1.6 - Computers and Network Devices - Device Locking
44	Security Update Management-1 - Security Update Management
45	Security Update Management-1.1 - Security Update Management - Licensed Software
46	Security Update Management-1.2 - Security Update Management - Unsupported Software
47	Security Update Management-1.3 - Security Update Management - Automatic Updates
48	Security Update Management-1.4 - Security Update Management - Critical Updates
49	User Access Control-1 - User Access Control
50	User Access Control-1.1 - User Access Control - Account Creation and Approval
51	User Access Control-1.2 - User Access Control - User Authentication and Unique Credentials

52	User Access Control-1.3 - User Access Control - Remove or Disable Accounts
53	User Access Control-1.4 - User Access Control - Multi-Factor Authentication (MFA)
54	User Access Control-1.5 - User Access Control - Administrative Accounts
55	User Access Control-1.6 - User Access Control - Remove or Disable Special Access Privileges

Purpose

Software includes operating systems, commercial off-the-shelf applications, extensions, interpreters, scripts, libraries, network software and firewall and router firmware.

• Devices include 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 and remote working
The default approach is that all corporate or BYOD home and remote 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 or remote 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 or remote 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, 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.

Data Backup-1 - Data Backup - Recommended

UK Cyber Essentials - v3.2	Other Requirements
Data Backup-1 Data Backup - Recommended	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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

Guidance
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.

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

Related Internal Controls
- 2023.UKCE-51 - Data Backup - Recommended: Backing up means creating a copy of your information and saving it to another device or to cloud storage (online).

  Procedure
  - Create a copy of your information and save it to another device or to cloud storage (online).

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/

Device Unlocking Credentials-1 - Device Unlocking Credentials

UK Cyber Essentials - v3.2	Other Requirements
Device Unlocking Credentials-1 Device Unlocking Credentials	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Where a device requires the physical presence of a user to gain access to the services the device offers (e.g., laptop logon, mobile phone unlock) the user must unlock the device using a credential such as a biometric, password or PIN before gaining access to the services.

Guidance
Devices should be protected against access by unauthorized users.

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

Related Internal Controls

- 2023.UKCE-15 - Device Unlocking Credentials: Where a device requires the physical presence of a user to gain access to the services the device offers (e.g., laptop logon, mobile phone unlock) the user must unlock the device using a credential such as a biometric, password or PIN before gaining access to the services.

  Procedure
  - Set devices to be unlocked using a credential such as a biometric, password or PIN before gaining access to the 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/

Device Unlocking Credentials-1.1 - Device Unlocking Credentials - Brute Force Attack Prevention

UK Cyber Essentials - v3.2	Other Requirements
Device Unlocking Credentials-1.1 Device Unlocking Credentials - Brute Force Attack Prevention	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Biometric tests, passwords and PINs must be protected against brute-force attack by at least one of:
• 'Throttling' the rate of attempts. This means the time the user must wait between attempts increases with each unsuccessful attempt. This should permit no more than 10 guesses in 5 minutes.
• Locking devices after no more than 10 unsuccessful attempts.

Guidance
Brute force attacks are when hackers use trial-and-error methods to crack passwords, login credentials, and encryption keys.

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

Related Internal Controls
- 2023.UKCE-16 - Device Unlocking Credentials - Brute Force Attack Prevention:
  Biometric tests, passwords and PINs must be protected against brute-force attack by at least one of:
  - 'Throttling' the rate of attempts. This means the time the user must wait between attempts increases with each unsuccessful attempt. This should permit no more than 10 guesses in 5 minutes.
  - Locking devices after no more than 10 unsuccessful attempts.

  Procedure
  - Throttle' the rate of attempts by increasing the time the user must wait between attempts with each unsuccessful attempt. This should permit no more than 10 guesses in 5 minutes. Lock devices after no more than 10 unsuccessful attempts

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/

Device Unlocking Credentials-1.2 - Device Unlocking Credentials - Technical Controls

UK Cyber Essentials - v3.2	Other Requirements
Device Unlocking Credentials-1.2 Device Unlocking Credentials - Technical Controls	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Technical controls must be used to manage the quality of credentials. If credentials are solely to unlock a device a minimum password or PIN length of at least 6 characters must be used. When the device unlocking credentials are used elsewhere, then the full password requirements in user access control must be applied to the credentials.

Guidance
The shorter and simpler a password or login credential, the easier it is to crack.

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

Related Internal Controls

- 2023.UKCE-17 - Device Unlocking Credentials - Technical Controls: Technical controls must be used to manage the quality of credentials. If credentials are solely to unlock a device a minimum password or PIN length of at least 6 characters must be used. When the device unlocking credentials are used elsewhere, then the full password requirements in “user access control” must be applied to the credentials.

  Procedure
  - If credentials are solely to unlock a device set a minimum password or PIN length of at least 6 characters. When the device unlocking credentials are used elsewhere, then the full password requirements in “user access control” must be applied to the credentials.

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/

Firewalls-1 - Properly Configured Firewall

UK Cyber Essentials - v3.2	Other Requirements
Firewalls-1 Properly Configured Firewall	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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, laptops, 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, 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.

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

Related Internal Controls
- 2023.UKCE-1 - Properly Configure Firewall(s): Protect all in-scope devices with a properly-configured firewall.

  Procedure
  - Deploy firewalls configured by qualified technicians.

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/

Firewalls-1.1 - Change Firewall Password or Disable Remote Administration

UK Cyber Essentials - v3.2	Other Requirements
Firewalls-1.1 Change Firewall Password or Disable Remote Administration	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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

- 2023.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.

  Procedure
  - Change firewall default administrative passwords or disable remote administrative access.

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/

Firewalls-1.2 - Prevent Internet Administrative Access

UK Cyber Essentials - v3.2	Other Requirements
Firewalls-1.2 Prevent Internet Administrative Access	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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

- 2023.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.

  Procedure
  - Prevent Internet access to the firewall or enable Multi-Factor Authentication (MFA), 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/

Firewalls-1.3 - Block Unauthenticated Inbound Connections

UK Cyber Essentials - v3.2	Other Requirements
Firewalls-1.3 Block Unauthenticated Inbound Connections	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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
- 2023.UKCE-4 - Block Unauthenticated Inbound Connections: For all firewalls (or equivalent network devices), the organisation must routinely block unauthenticated inbound connections by default.

  Procedure
  - Block unauthenticated inbound connections by default at the 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/

Firewalls-1.4 - Approve and Document Firewall Rules

UK Cyber Essentials - v3.2	Other Requirements
Firewalls-1.4 Approve and Document Firewall Rules	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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

- 2023.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.

  Procedure
  - 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/

Firewalls-1.5 - Remove or Disable Unnecessary Rules

UK Cyber Essentials - v3.2	Other Requirements
Firewalls-1.5 Remove or Disable Unnecessary Rules	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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
- 2023.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.

  Procedure
  - 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/

Firewalls-1.6 - Software Firewall

UK Cyber Essentials - v3.2	Other Requirements
Firewalls-1.6 Software Firewall	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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

- 2023.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.

  Procedure
  - 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/

Malware Protection-1 - Malware Protection

UK Cyber Essentials - v3.2	Other Requirements
Malware Protection-1 Malware Protection	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Restrict execution of known malware and untrusted software to prevent harmful code from causing damage or accessing sensitive data.

The execution of software downloaded from the Internet can expose a device to malware infection. Malware, such as computer viruses, worms and spyware, is software that has been written and distributed deliberately to perform malicious actions. Potential sources of malware infection include malicious email attachments, downloads (including those from application stores), and direct installation of unauthorised software.

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

Guidance
Applies to: Servers, desktop computers, laptops, tablets, mobile phones, IaaS, PaaS, SaaS

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

Related Internal Controls

- 2023.UKCE-43 - Malware Protection:
  Restrict execution of known malware and untrusted software, to prevent harmful code from causing damage or accessing sensitive data.

  The execution of software downloaded from the Internet can expose a device to malware infection. Malware, such as computer viruses, worms and spyware, is software that has been written and distributed deliberately to perform malicious actions. Potential sources of malware infection include malicious email attachments, downloads (including those from application stores), and direct installation of unauthorised software.

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

  Procedure
  - Restrict execution of known malware and untrusted software to prevent harmful code from causing damage or accessing sensitive data.

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 Document