METHOD

Cyber Essentials Checklist

Our free in-depth checklist gives an overview of the key measures you must be able to prove during the assessment process.

Cyber Essentials Checklist

Below is a short summary of each of the five key requirement areas, as well as a short checklist of the things you must prove to become certified.

Firewalls

A firewall ensures only safe and necessary network services can be accessed online. By restricting access, you reduce your exposure risk. Businesses must prove:

- ○ Firewalls have been correctly implemented on relevant devices
- ○ Appropriate settings have been configured
- ○ Software firewalls have been installed where appropriate

Secure Configuration

Servers, computers and other network devices must be properly configured to reduce vulnerabilities. Businesses must prove:

- ○ Secure user management
- ○ Authentication protocols are in place
- ○ Irrelevant software has been removed

User Access Control

User accounts must be tightly controlled, with access limited to the day-to-day requirements of users. Businesses must prove:

- ○ They have administrative control of all user accounts
- ○ Authentication procedures are in place
- ○ A process for removing access privileges exists

Malware Protection

Malware and untrusted software should be avoided, detected and removed to prevent harmful code from accessing or damaging sensitive data. Businesses must prove:

- ○ A malware protection strategy is in place
- ○ Sufficient scans are made of downloads and websites
- ○ An application approval process exists

Security Update Management

Devices and software must be updated regularly to ensure they are not vulnerable to known security issues. Businesses must prove:

- ○ A strategy to keep all software up to date exists
- ○ Updates are installed within a sufficient time frame
- ○ A software removal process is in place