inTEC EDUCATION

OUR WEBINAR WILL COMMENCE SHORTLY & WILL BE RECORDED

inTEC EDUCATION

Welcome

OWEN COLLAR:

Head of Cyber Security Audit
& Lead Assessor of the Cyber Essentials Scheme

CERTIFICATION BODY CYBER ESSENTIALS PLUS

CERTIFICATION BODY CYBER ESSENTIALS

CERTIFICATION BODY IASME GOVERNANCE

Gold Microsoft Partner

Microsoft

UKAS ISO 9001 QUALITY MANAGEMENT

Education Technology Specialists

- 20+ years experience of independent schools, MATs, maintained and special schools
- IT services that enable quality, innovation and excellence in education
- Agile and flexible, allowing us to deliver tailored and comprehensive IT solutions
- Proactive IT and infrastructure support

Education Technology Specialists

DIGITAL TRANSFORMATION

MANAGED IT SUPPORT SERVICES

INFRASTRUCTURE AND CLOUD SOLUTIONS

CYBER SECURITY AND SAFEGUARDING

What is Cyber Essentials?

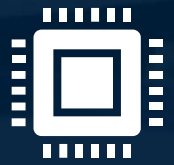
Cyber Essentials scheme is a UK government-backed initiative that helps organisations to protect themselves against common cyber threats.

5 key technical controls

1. Boundary firewalls and internet gateways
2. Secure configuration
3. Access control
4. Malware protection
5. Patch management

Cyber Essentials – the key changes

Grace periods extended to April 2023



Firmware clarification

Third party devices clarification

Device Unlocking update

Malware Protection update

Zero Trust guidance

Asset Management guidance

Grace periods extended to April 2023

- Cloud Services and MFA
- Thin clients will need to be listed
- Unsupported software needs to be removed

Firmware clarification

- Only Firewall and Router Firmware
- If a device can run a supported Operating System, this is sufficient. The Firmware is no longer required to be in support, apart from a Firewall or Router which must remain in support and declared within the scope
- User Devices will be reworded to: -
  - *"Cyber Essentials will require that all applicants list their laptops, desktops, servers, computers, tablets and mobile phones, with details of the make and operating system. However, when it comes to firewalls and routers, the applicant will only be asked to list make and model, but not the specific version of the firmware"* - which no longer requires checking by the assessor

Third party devices clarification

inTEC EDUCATION

	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	☑	☒	☒

Third party devices clarification

"Where devices are not in scope of the assessment, the school or organisation is still responsible for confirming that the devices accessing organisational services and data are configured correctly, but how this is achieved is up to them as it falls outside of the scope of the assessment."

Device unlocking update

- Brute force requirements for device unlocking
- Vendors defaults.

Malware protection update

- Anti-Malware software no longer needs to be signature-based
- Sandboxing has been removed from the anti-malware section

Zero Trust guidance

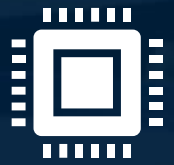
- Implementing the Cyber Essentials controls, will not prevent them from adopting the Zero Trust model.
- There is a direct correlation between Cyber Essentials and the NCSC Zero Trust model

Asset Management guidance

- Complements all five technical controls of Cyber Essentials
- Understand which devices are owned by an organisation

Cyber Essentials – Summary

Grace periods extended to April 2023



Firmware clarification

Third party devices clarification

Device Unlocking update

Malware Protection update

Zero Trust guidance

Asset Management guidance

Contact us for advice

CHAT: with your inTEC EDUCATION representative

EMAIL: enquiries@inteceducation.com

CALL: 0330 555 5550

VISIT: inteceducation.com/secureschools

Any questions?

Discover more at:
inteceducation.com