IT Installation and Cyber Essentials Implications

This document aims to support you in considering the potential security implications of IT installations.
Ongoing installations are an essential part of providing and improving services to pupils and staff. More recently, schools have been purchasing and installing new systems to meet the requirements and demands of remote learning. These installations have often been implemented at significant speed and with potential security implications.

There are many types of IT Installations which may have security implication including:

- WiFi installation.
- Network installation.
- Projector and whiteboard installation.

(Interactive boards which connect to the internet directly have security implications).

- Server installation (on-site or virtualised).
- Computer suite installation.
- Installing laptop trolleys.
- Mobile devices (tablets such as iPads).
- Software deployment.

Third Party Provision

Third parties may include cloud hosts, cloud-based software solutions, suppliers, technicians and installation engineers. In order to provision new services, third party providers may require access to existing systems.
Be sure that responsibilities during a project are clearly defined and that the responsibility of the school and any third-party are well understood and documented.
Consider how you will ensure that third parties will comply with school policies and procedures. Schools must ensure that providers are aware of business needs and security expectations.

Consider the Risks

Change management is vital to make sure that processes are followed, suitable training takes place and that security risks are understood and reduced to a minimal level.
Security risk assessments and a Data Protection Impact Assessments (DPIAs) should consider the risks of the following:

1. Equipment damage
2. Data loss
3. Data corruption
4. Service loss or interruption
5. Harm to personnel during installation
6. Damage to property

Cyber Essentials and Installations

New installations may overlap with Cyber Essentials requirements in the following ways:

1. You will need to change the default password on all firewalls and routers after installation to a unique, difficult to guess password at least 8 characters in length. (*Section 4 – Boundary Protection*)

2. You will need to ensure that all services that are being advertised from your router to the internet (open ports) are closed. If you need to open ports for a specific reason there must be a business case to support this. *(Section 4 - Boundary Protection)*

   For the purpose of Cyber Essentials, **a business case** means a decision which is signed off at board level by governors or trustees. When signing off, the board must consider the likelihood and impact of any risks relating and consider a review date.

3. If you have a business case for open services, ensure there is a process for disabling them when they are no longer required open. *(Section 4 - Boundary Protection)*

4. Ensure that your internet routers or hardware firewalls cannot be configured via the internet. If they can be, you will need to have a supporting business case and 2FA enabled or only allow access from trusted IP addresses. *(Section 4 – Boundary Protection)*

5. Where software firewalls are available, they should be enabled and configured on all computers and laptops. (*Section 4 – Boundary Protection*)

6. Make sure default passwords are changed to unique passwords of at least 8 characters on all devices including servers and mobile devices. *(Section 5 – Secure Configuration)*

7. Ensure all unused software, applications and unused accounts on new computers (example Guest Account) are removed. *(Section 5 – Secure Configuration)*

8. If your new installation runs software that provides sensitive information externally to the internet ensure that you apply the correct password policies including password throttling (restricting unsuccessful attempts) and have a policy to guide users including what to do if they believe they have been compromised, *(Section 5 – Secure Configuration)*

9. Disable auto-run or auto-play from your new systems. *(Section 5 – Secure Configuration)*

10. If a software installation replaced an older package, ensure historic packages are uninstalled. Secure any data from the old system or confirm secure data deletion from old systems, if required. *(Section 6 – Patch Management)*

11. Understand how any new system will be updated to ensure on-going security compliance and enable automatic updates to your Operating system and apps, If automatic updates are not possible, ensure you have a procedure to ensure all security patches are applied within 14 days. *(Section 6 – Patch Management)*

12. Ensure you understand the lifecycle of the Operating System and apps on your new installation and record when it will no longer be supported by the vendor. *Section 6 – Patch Management)*

13. Ensure you have updated records, such as the software and hardware inventories, asset registers, administrator log and relevant policies. *(Section 5 - Secure Configuration and Section 7 – User Access)*
14. User accounts must be created by following an approval process. Any administrative accounts should be created with an audit trail of the request and approval and confirmation of the access given. *(Section 7 – User Access)*

15. Consider whether implementation will require the installer to have additional access / admin rights. If so, ensure any additional rights are revoked at the end of the process. *(Section 7 – User Access)*

16. Ensure those with administrator access are correctly trained for the role and ensure that they are aware of the importance of segregated duties. They should not use their elevated accounts for every-day tasks e.g. web browsing / emails. (*Section 7 – User Access)*

17. Ensure all those with Administrator level accounts have 2FA enabled *where it is available. (*Section 7 – User Access)*

18. Ensure that you have adequate Malware protection in place on your devices, through an anti-malware software, using a trusted application list or sandboxing. *(Section 8 – Malware)*
    Sandboxing is the process of testing out new software in a segregated environment away from your school's network before introducing it.

19. If Anti-Malware is installed, ensure it is set to update at least daily and scan files automatically as well as providing web browsing protection. (scan and warn web pages you visit).

20. If new software is being rolled out, check that testing has taken place, has application sandboxing been used, and, ultimately, has it been added to authorised software lists? *(Section 8 – Malware)*

Failure to apply suitable mitigations and/or procedures could invalidate any cyber insurance.

Associated Legislation (https://www.legislation.gov.uk/)

Data Protection Act 2018 and the **UK GDPR** which covers all aspects of data protection.
The **Network and Information Systems Regulations 2018** which aims to address the threats posed to network and information systems.
Health and Safety at Work Act (1974) which puts a responsibility upon employees to keep the workplace safe.
The Electricity at Work Regulations of 1989, Provision and Use of Work Equipment regulations of 1998.
Waste Electrical and Electronic Equipment (WEEE) Regulations 2013, which will apply to the decommissioning and disposal of any old equipment.
The Electricity at Work Regulations 1989, relating to portable appliance testing (PAT) may also be required one year after implementation.