SUMMIT Qualifications UK

Bring Your Own Device Guidence

There are different approaches to facilitate home working each of which have their own security considerations.

Company issued devices

This is generally the most secure option, but it is also the most expensive.

Things you should consider:

- Ensure that the devices can be supported and updated remotely.
- Ensure that mechanisms are in place to prevent data from being exfiltrated from the device, eg data loss prevention technology.
- Ensure that remote access authentication is securely configured and consider using multi-factor authentication for remote access.

Use your own device, but access company software

This is a more cost-effective option, but comes with some security risks.

Things you should consider:

- Consider using multi-factor authentication for remote access.
- The device owner's data and the organisation's data should be separate. Staff should not be able to inadvertently or deliberately move the organisation's data into their personal storage on the device or onto separate personally-owned devices.
- Organisations need to be aware that the device's security posture may be compromised and plan accordingly, eg out of date and unpatched operating system or security software.

Use your own device

This approach has the most security risks and should be avoided for all but the smallest organisations with an immediate need to work remotely with no other remote working capability.

Things you should consider:

- Out of date software (including the operating system) may be vulnerable to exploitation including loss or compromise of personal data.
- Devices are likely to be shared between family members. Other family members may see personal data that they should not have access to.
- Data is unlikely to be encrypted on the device and may be vulnerable in the event of loss or theft of the device.

- Inadequate access control, eg weak laptop passwords, may result in personal data being easy for unauthorised individuals to access.
- Data can easily be moved to other insecure storage (personally-owned USB sticks and external hard drives), increasing the potential for loss.
- Staff usage of insecure methods to communicate, such as personal email accounts, may result in compromise of personal data.

What are the responsibilities of employees and employers when using BYOD?

Employers must set clear standards on how private devices may be used for corporate purposes. The following employee responsibilities must be governed in the employment context:

- The operating system must be updated regularly, because the updates for smartphones and tablets bridge security gaps.
- Apps must also be updated regularly so that they do not become a gateway for malware.
- Only the apps authorised by the company should be used for work tasks, since unauthorised apps carry a high data protection risk.
- Security mechanisms must be established for open WLAN networks that are not necessarily secure.
- The operating system configured by the manufacturer should not be modified, as this would make the file system open to attack.
- Company data should only be accessed via a secured browser, as otherwise malware could infiltrate the system.