TECHDUDS2

Implement security for a digital device

Overview

This standard is about protecting a digital device by implementing security controls.

It involves implementing own password protection to devices and configuring security software running on devices. It includes implementing data backup software to maintain copies of file structures and data and testing the ability to recover data should that be required. It also includes keeping operating system software up to date and removing unused software to reduce risks.

This standard is for those who need to implement security for digital devices to meet their own needs or as part of their duties.

Performance criteria

You must be able to:

1. Establish processes for implementing and updating strong password protection on digital devices in line with organisational standards
2. Implement, configure and maintain antivirus security software to protect from threats to privacy and data on digital devices in line with organisational standards
3. Run antivirus security scans on digital device to identify security issues in line with organisational procedures
4. Check all external drives to a digital device with security software before use and restrict access to drive ports that are not used in line with organisational procedures
5. Implement backup and recovery solutions to safeguard data in line with organisational procedures
6. Perform periodic data backups using manual or automated procedures in line with organisational standards
7. Test data backup and recovery solutions deliver the correct functionality
8. Keep operating system and application software up to date in line with organisational software updating and patching policies
9. Remove unused drivers and software from digital devices to reduce cyber security risks
10. Identify and report any suspicious activity when using digital devices in line with organisational procedures

Knowledge and understanding

You need to know and understand:

1. What is meant by a data security breach
2. The main causes of data security breaches
3. The impact that computer viruses, malware and unauthorised access can have on digital systems and data to an organisation
4. How to recognise problems that may be caused by a computer virus, malware or unauthorised use of digital devices
5. How to report breaches caused by computer virus, malware or unauthorised use of digital devices
6. The legal and ethical obligations around storing and sharing personal and business data
7. The reporting requirements for data protection legislation
8. How to use built-in operating system security features
9. How to implement and test backup and recovery software
10. The need to keep operating system and application software up to date to maintain resilience
11. How to check for operating system and application software updates
12. The importance of checking all externally connected drives and devices to maintain resilience
13. How to run security scans on external devices

TECHDUDS2

Implement security for a digital device

Developed by	e-skills
Version Number	1
Date Approved	30 Mar 2022
Indicative Review Date	30 Mar 2025
Validity	Current
Status	Original
Originating Organisation	ODAG Consultants Ltd.
Original URN	TECHDUDS2
Relevant Occupations	ICT for Users
Suite	IT Users
Keywords	information security, data security, cyber security