Paper Code: FA-HNI2991

Level 2

# Hardware, Network and Infrastructure Foundation Apprenticeship - Mock Knowledge Test

## Information for registered centres

The seal on this examination paper must only be broken by the candidate at the time of the examination.

**Under no circumstances should a candidate use an unsealed examination paper.**

## Information for candidates

**Under no circumstances should you, the candidate, use an unsealed examination paper.**
This examination consists of **20 multiple-choice** questions.
The minimum pass mark is **12 correct answers.**
The duration of this examination is **60 minutes.**
You are **NOT** allowed any assistance to complete the answers.
You must use a pencil to complete the answer sheet - pens must **NOT** be used.
When completed, please leave the **examination answer sheet (EAS)** on the desk.

**EXAMINATION ANSWER SHEET (EAS) INSTRUCTIONS:**
For each question, fill in **ONE** answer **ONLY.**
If you make a mistake, ensure you erase it thoroughly.
You must mark your choice of answer by shading in **ONE** answer circle only.
Please mark each choice like this:

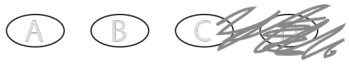

**ANSWER COMPLETED CORRECTLY**

**Examples of how NOT to mark your examination answer sheet (EAS). These will not be recorded.**


**DO NOT** partially shade the answer circle
**ANSWER COMPLETED INCORRECTLY**


**DO NOT** use ticks or crosses
**ANSWER COMPLETED INCORRECTLY**


**DO NOT** use circles
**ANSWER COMPLETED INCORRECTLY**




**DO NOT** shade over more than one answer circle
**ANSWER COMPLETED INCORRECTLY**

All candidates **MUST** sign the Examination Answer Sheet (EAS) in the bottom right-hand corner of the page before leaving the examination room.

**1**

The **main** goal of scams is to:

A. improve the performance of computer systems
B. increase awareness of cyber security policies
C. prevent access to restricted online services
D. trick people into giving away information

**2**

What is spyware designed to do on a computer system?

A. Block all unauthorised internet connections automatically
B. Protect files with stronger encryption methods
C. Secretly monitor user activity and collect information
D. Speed up the performance and connectivity of data applications

**3**

Why is cached data often cleared from a computer system?

A. To improve desktop appearance and personal settings
B. To keep files organised and reduce storage space usage
C. To remove stored details and prevent the misuse of information
D. To speed up browsing and increase internet connection

**4**

It is lawful for an organisation to use someone's personal data when:

A. the data is taken from a public website
B. the organisation already knows the person's email
C. the organisation wants to use it for marketing
D. the person has given clear consent for a specific reason

**5**

The purpose of a cyber security risk assessment is to:

A. decide which staff members are most likely to make mistakes
B. identify and prioritise any security risks before they occur
C. permanently remove all threats and dangers from the organisation
D. predict future cyber security risks against a business

**6**

One way to reduce eye strain when working on a computer is to:

A. keep the monitor brightness high to see clearly
B. place the monitor directly in front of a window to use natural light
C. position the screen at a comfortable distance
D. stare at the screen continuously when completing a task

**7**

Which of the following adjustments can be made to help prevent back strain at a workstation?

A. Aligning the chair to support the lower spine
B. Leaning forward to stretch the back while typing
C. Placing the screen at eye level to reduce neck pain
D. Sitting with the chair reclined away from the desk

**8**

Which of the following is a safe way to dispose of paper records containing personal information?

A. Placing the files in regular office recycling bins
B. Removing them from the office to dispose of them at home
C. Storing them in a cabinet and checking if they are needed later
D. Using shredding and an approved disposal service

**9**

Which of the following situations is an example of a malware infection?

A. A laptop slowing down after running out of storage
B. A server shutting down because it is overheating
C. A system becoming unusable after a ransomware attack
D. A website loading slowly due to heavy internet traffic

**10**

Outdated software creates a security risk because it:

A. makes programs harder for staff to understand
B. may contain known flaws that attackers can exploit
C. reduces the amount of data that systems can store
D. slows down computer processing during busy periods

**11**

How can the risk of adware be reduced?

A. Avoid adverts that appear during normal browsing
B. Install trusted security software on devices
C. Switch internet browsers on a regular basis
D. Use VPN services from unverified providers

**12**

Who typically performs penetration testing for an organisation?

A. Anyone with permission to browse company websites or data
B. Employees from any department who have experience in testing
C. Internal or external specialists trained in ethical hacking
D. Regular staff with access to all company system testing

**13**

Which of the following is an example of an unpatched system?

A. A device running software that no longer has vendor support
B. A program updated automatically through cloud services
C. A server that only allows manual installation of updates
D. A system with security updates available but not installed

**14**

What is the **main** risk of using weak encryption on sensitive data?

A. Attackers can break the protection and read the data
B. Data may take longer to upload to the internet
C. Files may be harder for employees to store and locate
D. Staff may need to change their passwords more often

**15**

What is the **main** purpose of remote access control?

A. To increase the speed of internet connections
B. To reduce the number of passwords staff need to remember
C. To remove the need for passwords on work devices
D. To restrict who connects to systems off-site

**16**

A common goal of a denial of service (DoS) attack is to:

A. disrupt services by overwhelming systems with traffic
B. force staff to share their passwords by impersonating IT
C. install ransomware that encrypts confidential files
D. permanently delete all company data from its servers

**17**

Which of the following is a common form of phishing?

A. Asking staff to complete routine hardware training
B. Installing official security patches onto hardware
C. Running regular anti-virus scans on company systems
D. Sending fake emails that appear to be genuine

**18**

What does the term insider threat mean in cyber security?

A. A current or former employee misusing authorised access
B. A fault in hardware that causes system failure
C. A hacker from another country breaking into systems
D. A virus that spreads through infected email attachments

**19**

What is the purpose of restricting the use of password managers?

A. To avoid having to change passwords regularly
B. To ensure staff remember every password manually
C. To prevent employees from creating long passwords
D. To reduce the risk of passwords being accessed in one place

**20**

Organisational procedures require that hazards are reported promptly so that:

A. action can be taken before anyone is harmed
B. managers have a written record for future reference
C. staff can prove they followed the correct process
D. the issue can be discussed in the next team meeting

Level 2

**Highfield Qualifications**

Highfield ICON
First Point
Balby Carr Bank
Doncaster
South Yorkshire
DN4 5JQ
United Kingdom

**01302 363277**
**info@highfield.co.uk**
**www.highfieldqualifications.com**