Paper Code: FA-HNI2992

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

What does the term malware mean?

A. Software that improves computer storage size
B. Software that is created for entertainment purposes
C. Software that is designed to damage systems
D. Software that is only used for office communication

2

Which of the following describes a denial of service (DoS) attack?

A. A deliberate overload of systems to make them unavailable to users
B. A phishing attempt that tricks users into revealing login details
C. A scam involving fake invoices sent to company email addresses
D. A security audit carried out by a trusted third-party organisation

3

Which of the following actions supports maintaining wellbeing while working at a computer?

A. Adjusting screen brightness to the highest level for viewing clarity
B. Keeping feet flat on the floor with the correct back posture
C. Positioning the monitor at a sharp angle to avoid glare
D. Resting forearms on the edge of the desk for stability

4

Which of the following is classed as personal data under the General Data Protection Regulation (GDPR)?

A. Information about company money and accounts
B. Information an organisation creates for its own use
C. Information that can identify a person directly or indirectly
D. Information that is written and printed in paper records only

5

Which of the following measures improves the security of remote access?

A. Allowing staff to share accounts for flexibility
B. Removing encryption from off-site connections
C. Requiring multi-factor authentication for logins
D. Using public Wi-Fi networks for connectivity

6

What is the **first** step if smoke or fire is noticed in the workplace?

A. Activate the fire alarm before leaving the area
B. Look for a manager before taking any action
C. Move equipment to a safe area before evacuating
D. Wait for confirmation of a fire before alerting others

7

Fraudulent phone calls are often used in phishing attacks to:

A. advertise new digital services and subscriptions
B. impersonate trusted people and request sensitive data
C. offer staff free technical training and support
D. test staff on company security policies and procedures

8

What makes an unpatched system vulnerable to attack?

A. It blocks all attempts to install critical updates
B. It has available security fixes that have not been installed
C. It has been replaced with a newer version by the vendor
D. It is too old to run modern software or tools

9

Why can unvetted VPNs expose users to adware?

A. They are slower than licensed VPNs
B. They may include hidden software that generates adverts
C. They often require stronger passwords than normal VPNs
D. They provide unlimited access to secure websites

10

What is the **main** purpose of the Network and Information Systems (NIS) Regulations?

A. To improve workplace wellbeing policies for staff
B. To provide training on using office software packages
C. To set standards for internet speed and access charges
D. To strengthen the security of essential services and providers

11

Which of the following is an example of weak encryption?

A. A document saved in a password-protected company drive
B. A file transferred over a secure VPN
C. A password stored with simple algorithms
D. An email sent using a system with two-factor authentication

12

The **main** purpose of penetration testing is to:

A. deliberately crash systems and test recovery speed
B. find security weaknesses before attackers can exploit them
C. permanently block staff from accessing data and systems
D. replace antivirus software with manual testing

13

Which of the following actions demonstrates compliance with cyber security policies?

A. Backing up company data to a personal cloud account
B. Checking a colleague's login details to help them complete urgent work
C. Following password rules and acceptable use procedures
D. Using the same username and password for all accounts

14

What is the **main** risk of relying too heavily on a password manager?

A. Employees may forget to delete inactive passwords
B. Passwords may be stored all in one place
C. Passwords may become longer than necessary
D. Staff may avoid changing passwords regularly

15

ID badges **must** be shown when employees are in the workplace to:

A. confirm identity and control access
B. display identity and show job roles
C. improve teamwork and build morale
D. record hours and track attendance

16

Which of the following is a typical sign that spyware is installed on a device?

A. Faster internet speeds during work hours
B. Improved battery life on a mobile device
C. New software updates arriving earlier than expected
D. Unexpected pop-ups running in the background

17

A **key** reason for following health and safety policies in a workplace is to:

A. ensure managers are not solely responsible for accidents
B. minimise the length of training so staff can focus on tasks
C. reduce the risk of accidents and injuries for all staff members
D. rely on skills and experience rather than formal safety guidance

18

Why **must** people be cautious when asked to download files unexpectedly?

A. It may contain malicious software
B. It may make internet browsing less efficient
C. It may reduce computer speed temporarily
D. It may remove old files automatically

19

The role of colleague whistleblowing in workplace security is to:

A. encourage teamwork and support social activities
B. monitor staff punctuality and record completed work
C. report unsafe and dishonest practices to management
D. track equipment use and check stock levels

20

Which of the following typically increases the risk of introducing malware?

A. Encrypting USB drives that contain sensitive project data
B. Restricting external storage device access on company laptops
C. Scanning removeable devices before connecting to company machines
D. Using personal USB drives to transfer files between multiple devices

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