Paper Code: FA-SDT2991

Level 2

Software and Data 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:

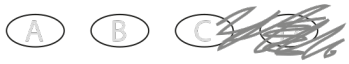
ANSWER COMPLETED CORRECTLY

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

Which of the following is a secure way to delete sensitive data that is no longer needed?

A. Removing files from folders and emptying the recycle bin
B. Renaming the files and moving them to an archive folder
C. Saving the files to a personal drive before deleting them
D. Wiping or overwriting files using approved deletion tools

2

What is the **main** purpose of a data retention policy?

A. To guide teams on when to move records from active use to archives
B. To provide rules for how records must be classified by importance
C. To reduce storage risks by reviewing data regularly for removal
D. To specify how long data can be kept to meet legal needs

3

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

4

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

A. keep the screen 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

5

Why is sharing login details with colleagues a security risk?

A. It automatically locks accounts after multiple logins
B. It encrypts account information and makes it unreadable
C. It prevents staff from accessing unauthorised files and documents
D. It removes the ability to track who accessed a system

6

Which of the following is the correct way to protect confidential data on shared devices?

A. Leaving files open and logged in for quick access by colleagues
B. Logging out and storing documents on secure systems
C. Saving documents locally and backing them up to a personal USB
D. Sharing passwords and instructions with team members for convenience

7

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

8

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

9

How can critical data be protected against loss?

A. By backing up data regularly to company-approved secure storage
B. By keeping a single copy of data on a secure internal drive
C. By relying on memory and recreating data if it is deleted accidentally
D. By using informal back-up data and copies saved on personal devices

10

Which of the following describes a distributed denial of service (DDoS) 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

11

How are permissions for sensitive files typically assigned?

A. They are based on who has been in the company the longest
B. They are given to anyone who requests access to view a document
C. They are granted to entire departments before reviewing individual roles
D. They are limited to users who require access to perform their role

12

Which of the following is considered good practice when naming work files?

A. Adding version numbers to names only after a project is completed
B. Following consistent naming rules defined by the organisation
C. Naming files based on personal preferences for easy recall
D. Using short, random names to save time when creating files

13

Sharing work information through personal emails is a risk because:

A. emails can only be accessed from personal devices
B. personal accounts may lack company security controls
C. personal inboxes automatically delete all attachments
D. sending files by personal email makes them read-only by default

14

What is the appropriate action to take if an email is received that looks suspicious?

A. Delete the email immediately without informing anyone
B. Forward it to other colleagues to ask if it's genuine
C. Reply to the sender to confirm their identity before opening
D. Report the email through the organisation's phishing procedure

15

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

16

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

17

How can risks be addressed once they are identified?

A. By applying controls to reduce their impact
B. By disregarding risks with a low chance of occurring
C. By focusing on threats from outside the organisation
D. By sharing responsibility for risks with all staff

18

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 critical systems
D. replace antivirus software with manual testing

19

Which of the following signs may indicate that a message or call is part of a scam?

A. A call scheduled in advance through the company calendar system
B. A message from a company that has been defrauded recently
C. A request confirmed through an official ticketing system
D. A request for payment or data with a sense of urgency

20

Using outdated software is a risk because it:

A. automatically disables antivirus protection
B. makes systems run faster but less securely
C. may contain known issues that attackers can exploit
D. prevents systems from being used on older 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