KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **SC-730**

Title : Cybersecurity Business Professional (beta)

Version : DEMO

1.Your organization uses Microsoft 365 for daily business operations.
According to the cybersecurity shared responsibility model, which of the following tasks is exclusively the responsibility of the customer (you and your organization)?
A. Applying security patches to the underlying host operating systems.
B. Managing the physical security of the cloud provider's data centers.
C. Configuring the hypervisor software that isolates virtual machines.
D. Protecting account credentials and correctly classifying sensitive data.
Answer: D
Explanation:
In the shared responsibility model for cloud services (like SaaS), the cloud provider manages the physical infrastructure, network, and host operating systems. However, the customer is always responsible for protecting user identities (passwords, MFA) and correctly classifying/handling the data uploaded to the cloud.

2.Which of the following actions best demonstrates an employee's active participation in their organization's security awareness initiatives?
A. Completing mandatory training and reporting suspicious emails promptly.
B. Attempting to bypass the corporate firewall to test its overall security.
C. Purchasing and installing unapproved security software on your laptop.
D. Forwarding all internal company newsletters to a personal email address.
Answer: A
Explanation:
As a business professional, you are not expected to perform technical penetration testing (Option B) or install unapproved IT tools (Option C). Active participation means understanding policies, completing training, and using correct reporting channels when spotting potential threats like phishing.

3.Company policy strictly prohibits a team of marketing employees from logging into a third-party social media management tool using a single, shared login credential.
What is the primary reason for this rule?
A. It guarantees that the shared account will be immediately targeted by external actors.
B. It automatically disables the multifactor authentication for the entire corporate network.
C. It prevents the organization from tracing specific actions back to an individual user.
D. It significantly decreases the processing speed of the third-party software platform.
Answer: C
Explanation:
Accountability is a core cybersecurity practice. It ensures that every action taken on a system can be definitively tied to a specific individual. Shared accounts eliminate accountability, making it impossible to determine who exactly made a change, leaked data, or made an error.

4.Your team is evaluating a free, public generative AI tool to help write reports.
According to standard organizational data-handling policies, which type of data must NEVER be inputted into this tool?
A. General industry news articles published on public media websites.
B. Unreleased financial forecasts and proprietary business data.

C. A standard template used for out-of-office email auto-replies.
D. Publicly available marketing brochures from your company.
Answer: B
Explanation:
Free and public generative AI models often use user prompts to train their underlying systems. Inputting sensitive, unreleased, or proprietary business data into these tools can lead to severe data leakage and confidentiality breaches.

5.The IT department mandates the use of an approved enterprise password manager.
What is the primary security benefit of integrating this tool into your daily workflow?
A. It actively scans the computer's hard drive to detect and remove malicious software.
B. It automatically intercepts and deletes all phishing emails before they reach the inbox.
C. It completely removes the need to use multi-factor authentication across the network.
D. It generates, auto-fills, and securely stores highly complex passwords for every system.
Answer: D
Explanation:
A password manager solves "password fatigue." It prevents the dangerous practice of password reuse by generating strong, unique passwords for every application and storing them in an encrypted vault. It does not replace MFA or act as an antivirus.