



# CS0-001<sup>Q&As</sup>

CompTIA Cybersecurity Analyst

**Pass CompTIA CS0-001 Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.lead4pass.com/cs0-001.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA  
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





### QUESTION 1

A security analyst is concerned that employees may attempt to exfiltrate data prior to tendering their resignations. Unfortunately, the company cannot afford to purchase a data loss prevention (DLP) system. Which of the following recommendations should the security analyst make to provide defense-in-depth against data loss? (Select THREE).

- A. Prevent users from accessing personal email and file-sharing sites via web proxy
- B. Prevent flash drives from connecting to USB ports using Group Policy
- C. Prevent users from copying data from workstation to workstation
- D. Prevent users from using roaming profiles when changing workstations
- E. Prevent Internet access on laptops unless connected to the network in the office or via VPN
- F. Prevent users from being able to use the copy and paste functions

Correct Answer: ABE

---

### QUESTION 2

The service desk has received several calls from the remote workforce group stating they have experienced degradation in services. The security analyst discovers all the remote laptops have become infected with a known virus that was introduced by a known application weakness. Which of the following is the BEST course of action to ensure the remote workers do not experience this issue in the future?

- A. Communicate to the remote workers that company laptops are for work purposes only.
- B. Configure the devices to access the Internet through the corporate network only.
- C. Ensure devices receive software updates and definitions upon connecting to the internal network.
- D. Develop and configure a whitelist on each laptop for authored, business-related websites only.

Correct Answer: C

---

### QUESTION 3

Which of the following actions should occur to address any open issues while closing an incident involving various departments within the network?

- A. Incident response plan
- B. Lessons learned report
- C. Reverse engineering process
- D. Chain of custody documentation



Correct Answer: B

---

#### QUESTION 4

A security analyst has created an image of a drive from an incident. Which of the following describes what the analyst should do NEXT?

- A. The analyst should create a backup of the drive and then hash the drive.
- B. The analyst should begin analyzing the image and begin to report findings.
- C. The analyst should create a hash of the image and compare it to the original drive's hash.
- D. The analyst should create a chain of custody document and notify stakeholders.

Correct Answer: C

---

#### QUESTION 5

A computer at a company was used to commit a crime. The system was seized and removed for further analysis. Which of the following is the purpose of labeling cables and connections when seizing the computer system?

- A. To capture the system configuration as it was at the time it was removed
- B. To maintain the chain of custody
- C. To block any communication with the computer system from attack
- D. To document the model, manufacturer, and type of cables connected

Correct Answer: A

[Latest CS0-001 Dumps](#)

[CS0-001 Study Guide](#)

[CS0-001 Exam Questions](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

## Try our product !

100% Guaranteed Success  
100% Money Back Guarantee  
365 Days Free Update  
Instant Download After Purchase  
24x7 Customer Support  
Average 99.9% Success Rate  
More than 800,000 Satisfied Customers Worldwide  
Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.lead4pass.com/allproducts>

## Need Help

Please provide as much detail as possible so we can best assist you.  
To update a previously submitted ticket:



 <p><b>One Year Free Update</b> Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p><b>Money Back Guarantee</b> To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p><b>Security &amp; Privacy</b> We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information &amp; peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.  
All trademarks are the property of their respective owners.  
Copyright © lead4pass, All Rights Reserved.