CDPSE通過考試 - CDPSE下載

此外，這些PDFExamDumps CDPSE考試題庫的部分內容現在是免費的：https://drive.google.com/open?id=1g0tqQN3sULx68X7dkaOYLAQxff4LoCKx

如果你仍然在努力學習為通過ISACA的CDPSE考試認證，我們PDFExamDumps為你實現你的夢想。我們為你提供ISACA的CDPSE考試考古題，通過了實踐的檢驗，ISACA的CDPSE教程及任何其他相關材料，最好的品質，以幫助你通過ISACA的CDPSE考試認證，成為一個實力雄厚的IT專家。

對于CDPSE認證是評估職員在公司所具備的能力和知識，而如何獲得ISACA CDPSE認證是大多數考生面臨的挑戰性的問題。現在的考試如CDPSE在經常的跟新，準備通過這個考試是一項艱巨的任務，ISACA CDPSE考古題是一個能使您一次性通過該考試的題庫資料。一旦您通過考試，您將獲得不錯的工作機會，所以，選擇CDPSE題庫就是選擇成功，我們將保證您百分之百通過考試。

>> CDPSE通過考試 <<

有效的考試認證資料ISACA CDPSE通過考試是由ISACA公司專業認證培訓師認真研發的

PDFExamDumps為你提供了不同版本的資料以方便你的使用。PDF版的CDPSE考古題方便你的閱讀，為你真實地再現考試題目。軟體版本的CDPSE考古題作為一個測試引擎，可以幫助你隨時測試自己的準備情況。如果你想知道你是不是充分準備好了CDPSE考試，那麼你可以利用軟體版的考古題來測試一下自己的水準。這樣你就可以快速找出自己的弱點和不足，進而有利於你的下一步學習安排。

最新的 Isaca Certification CDPSE 免費考試真題 (Q45-Q50):

問題 #45
Which of the following is the BEST practice to protect data privacy when disposing removable backup media?

- A. Data scrambling
- B. Data encryption
- C. Data sanitization
- D. Data masking

答案：C

解題說明：
Explanation
The best practice to protect data privacy when disposing removable backup media is B. Data sanitization.
A comprehensive explanation is:
Data sanitization is the process of permanently and irreversibly erasing or destroying the data on a storage device or media, such as a hard drive, a USB drive, a CD/DVD, etc. Data sanitization ensures that the data cannot be recovered or reconstructed by any means, even by using specialized software or hardware tools.
Data sanitization is also known as data wiping, data erasure, data destruction, or data disposal.
Data sanitization is the best practice to protect data privacy when disposing removable backup media because it prevents unauthorized access, disclosure, theft, or misuse of the sensitive or confidential data that may be stored on the media. Data

sanitization also helps to comply with the legal and regulatory requirements and standards for data protection and privacy, such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), etc.
There are different methods and techniques for data sanitization, depending on the type and format of the storage device or media. Some of the common methods are:
* Overwriting: Overwriting replaces the existing data on the device or media with random or meaningless data, such as zeros, ones, or patterns. Overwriting can be done multiple times to increase the level of security and assurance. Overwriting is suitable for magnetic media, such as hard disk drives (HDDs) or tapes.
* Degaussing: Degaussing exposes the device or media to a strong magnetic field that disrupts and destroys the magnetic structure and alignment of the data. Degaussing renders the device or media unusable and unreadable. Degaussing is suitable for magnetic media, such as hard disk drives (HDDs) or tapes.
* Physical Destruction: Physical destruction involves applying physical force or damage to the device or media that breaks it into small pieces or shreds it. Physical destruction can be done by using mechanical tools, such as shredders, crushers, drills, hammers, etc., or by using thermal methods, such as incineration, melting, etc. Physical destruction is suitable for any type of media, such as hard disk drives (HDDs), solid state drives (SSDs), USB drives, CDs/DVDs, etc.
Data encryption (A) is not a good practice to protect data privacy when disposing removable backup media because it does not erase or destroy the data on the media. Data encryption only transforms the data into an unreadable format that can only be accessed with a key or a password. However, if the key or password is lost, stolen, compromised, or guessed by an attacker, the data can still be decrypted and exposed. Data encryption is more suitable for protecting data in transit or at rest, but not for disposing data.
Data scrambling is not a good practice to protect data privacy when disposing removable backup media because it does not erase or destroy the data on the media. Data scrambling only rearranges the order of the bits or bytes of the data to make it appear random or meaningless. However, if the algorithm or pattern of scrambling is known or discovered by an attacker, the data can still be unscrambled and restored. Data scrambling is more suitable for obfuscating data for testing or debugging purposes, but not for disposing data.
Data masking (D) is not a good practice to protect data privacy when disposing removable backup media because it does not erase or destroy the data on the media. Data masking only replaces some parts of the data with fictitious or anonymized values to hide its true identity or meaning. However, if the original data is still stored somewhere else or if the masking technique is weak or reversible by an attacker, the data can still be unmasked and revealed. Data masking is more suitable for protecting data in use or in analysis, but not for disposing data.
References:
* What Is Data Sanitization?1
* How to securely erase hard drives (HDDs) and solid state drives (SSDs)2
* Secure Data Disposal & Destruction: 6 Methods to Follow3

問題 #46
Which of the following is the MOST important privacy consideration when developing a contact tracing application?

- A. Whether the application can be audited for compliance purposes
- B. Retention period for data storage
- C. The creation of a clear privacy notice
- D. The proportionality of the data collected tor the intended purpose

答案：D

解題說明：
Explanation
The proportionality of the data collected for the intended purpose is the most important privacy consideration when developing a contact tracing application. This means that the application should only collect the minimum amount of personal data necessary to achieve the specific and legitimate purpose of preventing and controlling the spread of COVID-191. The application should also ensure that the data collected are relevant, adequate, and not excessive in relation to the purpose2. The application should avoid collecting or processing any data that are not essential for the purpose, such as location data, biometric data, or health data unrelated to COVID-193. The application should also respect the data minimization principle, which requires that the data are kept for no longer than necessary for the purpose4. References:
European Data Protection Board Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak Article 5(1) of the General Data Protection Regulation (GDPR) Article 29 Data Protection Working Party Opinion 04/2017 on the Proposed Regulation for the ePrivacy Regulation Article 5(1)(e) of the GDPR

問題 #47
Which of the following is the BEST practice to protect data privacy when disposing removable backup media?

- A. Data scrambling
- B. Data encryption
- C. Data sanitization
- D. Data masking

答案：C

解題說明：
Explanation
The best practice to protect data privacy when disposing removable backup media is B. Data sanitization.
A comprehensive explanation is:
Data sanitization is the process of permanently and irreversibly erasing or destroying the data on a storage device or media, such as a hard drive, a USB drive, a CD/DVD, etc. Data sanitization ensures that the data cannot be recovered or reconstructed by any means, even by using specialized software or hardware tools.
Data sanitization is also known as data wiping, data erasure, data destruction, or data disposal.
Data sanitization is the best practice to protect data privacy when disposing removable backup media because it prevents unauthorized access, disclosure, theft, or misuse of the sensitive or confidential data that may be stored on the media. Data sanitization also helps to comply with the legal and regulatory requirements and standards for data protection and privacy, such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), etc.
There are different methods and techniques for data sanitization, depending on the type and format of the storage device or media. Some of the common methods are:
Overwriting: Overwriting replaces the existing data on the device or media with random or meaningless data, such as zeros, ones, or patterns. Overwriting can be done multiple times to increase the level of security and assurance. Overwriting is suitable for magnetic media, such as hard disk drives (HDDs) or tapes.
Degaussing: Degaussing exposes the device or media to a strong magnetic field that disrupts and destroys the magnetic structure and alignment of the data. Degaussing renders the device or media unusable and unreadable. Degaussing is suitable for magnetic media, such as hard disk drives (HDDs) or tapes.
Physical Destruction: Physical destruction involves applying physical force or damage to the device or media that breaks it into small pieces or shreds it. Physical destruction can be done by using mechanical tools, such as shredders, crushers, drills, hammers, etc., or by using thermal methods, such as incineration, melting, etc. Physical destruction is suitable for any type of media, such as hard disk drives (HDDs), solid state drives (SSDs), USB drives, CDs/DVDs, etc.
Data encryption (A) is not a good practice to protect data privacy when disposing removable backup media because it does not erase or destroy the data on the media. Data encryption only transforms the data into an unreadable format that can only be accessed with a key or a password. However, if the key or password is lost, stolen, compromised, or guessed by an attacker, the data can still be decrypted and exposed. Data encryption is more suitable for protecting data in transit or at rest, but not for disposing data.
Data scrambling is not a good practice to protect data privacy when disposing removable backup media because it does not erase or destroy the data on the media. Data scrambling only rearranges the order of the bits or bytes of the data to make it appear random or meaningless. However, if the algorithm or pattern of scrambling is known or discovered by an attacker, the data can still be unscrambled and restored. Data scrambling is more suitable for obfuscating data for testing or debugging purposes, but not for disposing data.
Data masking (D) is not a good practice to protect data privacy when disposing removable backup media because it does not erase or destroy the data on the media. Data masking only replaces some parts of the data with fictitious or anonymized values to hide its true identity or meaning. However, if the original data is still stored somewhere else or if the masking technique is weak or reversible by an attacker, the data can still be unmasked and revealed. Data masking is more suitable for protecting data in use or in analysis, but not for disposing data.
References:
What Is Data Sanitization?1
How to securely erase hard drives (HDDs) and solid state drives (SSDs)2 Secure Data Disposal & Destruction: 6 Methods to Follow3

問題 #48
An organization is creating a personal data processing register to document actions taken with personal data.
Which of the following categories should document controls relating to periods of retention for personal data?

- A. Data input

- B. Data acquisition
- C. Data archiving
- D. Data storage

答案：C

解題說明：
Explanation
However, the risks associated with long-term retention have compelled organizations to consider alternatives; one is data archival, the process of preparing data for long-term storage. When organizations are bound by specific laws to retain data for many years, archival provides a viable opportunity to remove data from online transaction systems to other systems or media.
Data archiving is the process of moving data that is no longer actively used to a separate storage device for long-term retention. Data archiving helps to reduce the cost and complexity of data storage, improve the performance and availability of data systems, and comply with data retention policies and regulations. Data archiving should document controls relating to periods of retention for personal data, such as the criteria for determining the retention period, the procedures for deleting or anonymizing data after the retention period expires, and the mechanisms for ensuring the integrity and security of archived data. References: : CDPSE Review Manual (Digital Version), page 123

問題 #49
Which of the following poses the GREATEST privacy risk for client-side application processing?

- A. A remote employee placing communication software on a company server
- B. A distributed denial of service attack (DDoS) on the company network
- C. An employee loading personal information on a company laptop
- D. Failure of a firewall protecting the company network

答案：C

解題說明：
Explanation
The greatest privacy risk for client-side application processing is an employee loading personal information on a company laptop. Client-side application processing refers to performing data processing operations on the user's device or browser, rather than on a server or cloud. This can improve performance and user experience, but also pose privacy risks if the user's device is lost, stolen, hacked, or infected with malware. An employee loading personal information on a company laptop is exposing that information to potential threats on the client-side, such as unauthorized access, use, disclosure, modification, or loss. Therefore, an organization should implement appropriate security measures to protect personal information on client-side devices, such as encryption, authentication, authorization, logging, monitoring, etc. References: : CDPSE Review Manual (Digital Version), page 153

問題 #50
.....

CDPSE認證考試考古題 - 最新的ISACA CDPSE認證考試題庫

所有的免費試用產品都是方便客戶很好體驗我們題庫的真實性，你會發現 ISACA CDPSE 題庫資料是真實可靠的，競爭頗似打網球，與球藝勝過你的對手比賽，可以提高你的水準，是否能夠獲得70%或者以上得分？

- CDPSE題庫資訊 □ CDPSE真題材料 □ CDPSE最新考題 ✳ 打開【 tw.fast2test.com 】搜尋「 CDPSE 」以免費下載考試資料CDPSE考試指南
- CDPSE考題資源 □ CDPSE題庫資訊 □ CDPSE最新考題 □ 透過▹ www.newdumpspdf.com ◃搜索➥ CDPSE □免費下載考試資料CDPSE考試證照綜述
- 真實的CDPSE通過考試＆準確的ISACA認證培訓 - 有效的ISACA Certified Data Privacy Solutions Engineer □ ➠ tw.fast2test.com □提供免費（ CDPSE ）問題收集CDPSE真題材料
- CDPSE考題資源 ☯ CDPSE權威考題 □ CDPSE考試指南 □ 複製網址▹ www.newdumpspdf.com ◃打開並搜索" CDPSE "免費下載CDPSE考題免費下載
- 有效的CDPSE通過考試和資格考試中的領導者和非常好的ISACA Certified Data Privacy Solutions Engineer □ 在[www.pdfexamdumps.com]上搜索□ CDPSE □並獲取免費下載CDPSE考題
- 專業CDPSE通過考試及資格考試領先供應商和免費下載的ISACA Certified Data Privacy Solutions Engineer □ ➥ www.newdumpspdf.com □上的免費下載" CDPSE "頁面立即打開CDPSE考試證照綜述
- 專業CDPSE通過考試及資格考試領先供應商和免費下載的ISACA Certified Data Privacy Solutions Engineer □ 來自網站（ www.pdfexamdumps.com ）打開並搜索{ CDPSE }免費下載CDPSE題庫最新資訊
- 新版CDPSE考古題 □ 最新CDPSE考古題 □ 最新CDPSE試題 □ 透過《 www.newdumpspdf.com 》輕鬆獲取{ CDPSE }免費下載CDPSE題庫下載
- 準備充分的CDPSE通過考試和資格考試的領先材料提供商＆準確的CDPSE下載 □ 打開網站➤ www.vcesoft.com □搜索□ CDPSE □免費下載CDPSE考題
- CDPSE權威考題 □ CDPSE考古題分享 □ CDPSE考試指南 □ 透過□ www.newdumpspdf.com □搜索□ CDPSE □免費下載考試資料CDPSE最新考題
- 有效的CDPSE通過考試和資格考試中的領導者和非常好的ISACA Certified Data Privacy Solutions Engineer □ 在《 www.pdfexamdumps.com 》搜索最新的☀ CDPSE □☀□題庫CDPSE考試指南
- myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, s.258.cloudns.ch, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes

此外，這些PDFExamDumps CDPSE考試題庫的部分內容現在是免費的：https://drive.google.com/open?id=1g0tqQN3sULx68X7dkaOYLAQxff4LoCKx