CDPSE시험대비최신버전덤프시험준비에가장좋은인기시험자료

그리고 DumpTOP CDPSE 시험 문제집의 전체 버전을 클라우드 저장소에서 다운로드할 수 있습니다: https://drive.google.com/open?id=1VkZgu0jVhL_upec1qhOp3ubl8rfc5x-m

우리사이트가 다른 덤프사이트보다 우수한 점은 바로 자료들이 모두 전면적이고 적중률과 정확입니다. 때문에 우리DumpTOP를 선택함으로ISACA인증CDPSE시험준비에는 최고의 자료입니다. 여러분이 성공을 위한 최고의 자료입니다.

CDPSE 인증을 받으면 데이터 개인 정보 보호 및 효과적인 개인 정보 보호 솔루션을 관리하고 구현할 수있는 능력에 대한 강력한 약속이 나타납니다. 오늘날의 디지털 시대에는 데이터 개인 정보가 모든 규모와 산업의 조직에 중요한 관심사 인 오늘날의 디지털 시대에 점점 더 귀중한 인증입니다. CDPSE 시험을 통과함으로써 응시자는 전문적인 신뢰성을 높이고 IT 분야와 보안 분야에서 경력을 발전시킬 수 있습니다.

ISACA CDPSE (인증 데이터 프라이버시 솔루션 엔지니어) 자격증 시험은 조직에서 프라이버시 솔루션을 관리하고 구현하는 전문가의 전문성을 입증하고자 하는 전문가들을 위한 세계적으로 인정받는 자격증입니다. 이 자격증 시험은 프라이버시 프로그램을 효과적으로 관리하고 데이터 보호 솔루션을 구현하는 데 필요한 지식과 기술을 검증하기 위해 설계되었습니다. CDPSE 시험은 프라이버시 프로그램 지배 구조, 프라이버시 정책 및 절차, 프라이버시 위험 관리, 프라이버시 프로그램 운영화, 프라이버시 솔루션 구현 및 프라이버시 사고 관리 등 다양한 주제를 다룹니다.

CDPSE시험대비 최신버전 덤프 덤프로 Certified Data Privacy Solutions Engineer 시험을 패스하여 자격증 취득하기

DumpTOP의 ISACA CDPSE덤프는 IT업계에 오랜 시간동안 종사한 전문가들의 끊임없는 노력과 지금까지의 노하우로 만들어낸ISACA CDPSE시험대비 알맞춤 자료입니다. DumpTOP의 ISACA CDPSE덤프만 공부하시면 여러분은 충분히 안전하게 ISACA CDPSE시험을 패스하실 수 있습니다. DumpTOP ISACA CDPSE덤프의 도움으로 여러분은 IT업계에서 또 한층 업그레이드 될것입니다

ISACA CDPSE (Certified Data Privacy Solutions Engineer) 인증 시험은 데이터 개인 정보 및 보안을 전문으로하는 개인을위한 전 세계적으로 인정 된 인증입니다. CDPSE 인증 프로그램은 ISACA (Information Systems Audit and Control Association)에 의해 개발되고 관리됩니다. ISACA (Global Governance, Audit 및 Cybersecurity Professional의 주요 협회).

최신 Isaca Certification CDPSE 무료샘플문제 (Q248-Q253):

질문 # 248
Which of the following is the BEST way for an organization to gain visibility into Its exposure to privacy-related vulnerabilities?

- A. Perform an analysis of known threats.
- B. Implement a data loss prevention (DLP) solution.
- C. Review historical privacy incidents in the organization.
- D. Monitor inbound and outbound communications.

정답：A

설명：
Explanation
An analysis of known threats is the best way for an organization to gain visibility into its exposure to privacy-related vulnerabilities because it helps identify the sources, methods and impacts of potential privacy breaches and assess the effectiveness of existing controls. A data loss prevention (DLP) solution, a review of historical privacy incidents and a monitoring of inbound and outbound communications are useful tools for detecting and preventing privacy violations, but they do not provide a comprehensive view of the organization's privacy risk posture.
References:
CDPSE Review Manual (Digital Version), Domain 1: Privacy Governance, Task 1.4: Coordinate and/or perform privacy impact assessments (PIA) and other privacy-focused assessments1 CDPSE Certified Data Privacy Solutions Engineer All-in-One Exam Guide, Chapter 2: Privacy Governance, Section: Privacy Risk Assessment2

질문 # 249
Which of the following is the BEST way to protect the privacy of data stored on a laptop in case of loss or theft?

- A. Remote wipe
- B. Endpoint encryption
- C. Regular backups
- D. Strong authentication controls

정답：B

설명：
Endpoint encryption is a security practice that transforms the data stored on a laptop or other device into an unreadable format using a secret key or algorithm. Endpoint encryption protects the privacy of data in case of loss or theft, by ensuring that only authorized parties can access and use the data, while unauthorized parties cannot decipher or modify the data without the key or algorithm. Endpoint encryption also helps to comply with data protection laws and regulations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), which require data controllers and processors to implement appropriate technical and organizational measures to safeguard personal data.
The other options are less effective or irrelevant for protecting the privacy of data stored on a laptop in case of loss or theft. Strong authentication controls, such as passwords, biometrics or multifactor authentication, are important for verifying the identity and access rights of users, but they do not protect the data from being accessed by bypassing or breaking the authentication mechanisms. Remote wipe is a feature that allows users or administrators to erase the data on a lost or stolen device remotely, but it depends on

the availability of network connection and device power, and it may not prevent data recovery by sophisticated tools. Regular backups are a process of creating copies of data for recovery purposes, such as in case of data loss or corruption, but they do not protect the data from being accessed by unauthorized parties who may obtain the backup media or files.
Reference:
An Ethical Approach to Data Privacy Protection - ISACA, section 2: "Encryption is one of the most effective security controls available to enterprises, but it can be challenging to deploy and maintain across a complex enterprise landscape." How to Protect and Secure Your Data in 10 Ways - TechRepublic, section 1: "Encrypt your hard drive Most work laptops use BitLocker to encrypt local files. That way, if the computer is stolen or hacked, the data it contains will be useless to the malicious actor."
10 Tips to Protect Your Files on PC and Cloud - microsoft.com, section 1: "Encrypt your hard drive Most work laptops use BitLocker to encrypt local files. That way, if the computer is stolen or hacked, the data it contains will be useless to the malicious actor."
11 practical ways to keep your IT systems safe and secure | ICO, section 1: "Use strong passwords and multi-factor authentication Make sure you use strong passwords on smartphones, laptops, tablets, email accounts and any other devices or accounts where personal information is stored."

질문 # 250
What is the BES T way for an organization to maintain the effectiveness of its privacy breach incident response plan?
* Require security management to validate data privacy security practices.
* Conduct annual data privacy tabletop exercises

- A. Involve the privacy office in an organizational review of the incident response plan.
- B. Hire a third party to perform a review of data privacy processes.

정답：A

설명:
Explanation
The best way for an organization to maintain the effectiveness of its privacy breach incident response plan is to conduct annual data privacy tabletop exercises. A tabletop exercise is a simulated scenario that tests the organization's ability to respond to a privacy breach incident in a realistic and interactive way. A tabletop exercise can help the organization to evaluate the roles and responsibilities of the incident response team, identify the gaps and weaknesses in the plan, improve the communication and coordination among the stakeholders, and update the plan based on the lessons learned and best practices12. A tabletop exercise can also enhance the awareness and readiness of the organization to handle privacy breach incidents in a timely and effective manner3. References:
* ISACA CDPSE Review Manual, Chapter 4, Section 4.3.2
* ISACA Journal, Volume 4, 2019, "Tabletop Exercises: Three Sample Scenarios"
* ISACA Journal, Volume 6, 2017, "Privacy Breach Response: Preparing for the Inevitable"

질문 # 251
Which of the following is the MOST effective way to support organizational privacy awareness objectives?

- A. Customizing awareness training by business unit function
- B. Implementing an annual training certification process
- C. Funding in-depth training and awareness education for data privacy staff
- D. Including mandatory awareness training as part of performance evaluations

정답：A

설명:
Explanation
The most effective way to support organizational privacy awareness objectives is D. Customizing awareness training by business unit function.
A comprehensive explanation is:
Organizational privacy awareness objectives are the goals and expectations that an organization sets for its employees and stakeholders regarding the protection and management of personal data. Privacy awareness objectives may vary depending on the nature, scope, and purpose of the organization's data processing activities, as well as the legal, regulatory, contractual, and ethical obligations and implications that apply to them.
One of the best practices to support organizational privacy awareness objectives is to customize awareness training by business unit function. This means that the organization should design and deliver privacy awareness training programs that are tailored to the

specific roles, responsibilities, and needs of each business unit or department within the organization. Customizing awareness training by business unit function can have several benefits, such as:
* Enhancing the relevance and effectiveness of the training content and methods for each audience group, by addressing their specific privacy challenges, risks, and opportunities.
* Increasing the engagement and motivation of the trainees, by showing them how privacy relates to their daily tasks, goals, and performance.
* Improving the retention and application of the training knowledge and skills, by providing practical examples, scenarios, and exercises that reflect the real-world situations and problems that the trainees may encounter.
* Fostering a culture of privacy across the organization, by creating a common language and understanding of privacy concepts, principles, and practices among different business units or departments.
Some examples of how to customize awareness training by business unit function are:
* Providing different levels or modules of training based on the degree of access or exposure to personal data that each business unit or department has. For example, a basic level of training for all employees, an intermediate level of training for employees who handle personal data occasionally or incidentally, and an advanced level of training for employees who handle personal data regularly or extensively.
* Providing different topics or themes of training based on the type or category of personal data that each business unit or department processes. For example, a general topic of training for employees who process non-sensitive or non-personal data, a specific topic of training for employees who process sensitive or special data categories (such as health, biometric, financial, or political data), and a specialized topic of training for employees who process high-risk or high-value data (such as intellectual property, trade secrets, or customer loyalty data).
* Providing different formats or modes of training based on the preferences or constraints of each business unit or department. For example, a face-to-face format of training for employees who work in the same location or office, an online format of training for employees who work remotely or across different time zones, and a blended format of training for employees who work in a hybrid mode or have flexible schedules.
The other options are not as effective as option D.
Funding in-depth training and awareness education for data privacy staff (A) may improve the competence and confidence of the data privacy staff who are responsible for designing and implementing the privacy policies and practices of the organization, but it does not necessarily support the organizational privacy awareness objectives for the rest of the employees and stakeholders.
Implementing an annual training certification process (B) may ensure that the employees and stakeholders are updated and refreshed on the privacy policies and practices of the organization on a regular basis, but it does not necessarily address their specific privacy needs and challenges based on their business unit function.
Including mandatory awareness training as part of performance evaluations may incentivize the employees and stakeholders to participate in and complete the privacy awareness training programs offered by the organization, but it does not necessarily enhance their understanding and application of privacy concepts and principles based on their business unit function.
References:
* The Benefits of Information Security and Privacy Awareness Training Programs1
* What Is Your Privacy and Data Protection Strategy?2
* What is Data Privacy Awareness?3

질문 # 252
Which of the following is the BEST method of data sanitization when there is a need to balance the destruction of data and the ability to recycle IT assets?

- A. Data deletion
- B. Factory reset
- C. Cryptographic erasure
- D. Degaussing

정답：C

설명:
Explanation
Cryptographic erasure is a data sanitization method that uses encryption to render data unreadable and unrecoverable. It is the best method when there is a need to balance the destruction of data and the ability to recycle IT assets, because it does not damage the storage media and allows it to be reused or sold. It is also faster and more environmentally friendly than physical destruction methods.
References:
* ISACA Certified Data Privacy Solutions Engineer (CDPSE) Exam Content Outline, Domain 2: Privacy Architecture, Task 2.4: Implement data sanitization methods to ensure data privacy and security, Subtask 2.4.1: Select appropriate data sanitization methods based on the type of data and storage media.

* What is Data Sanitization? | Data Erasure Methods | Imperva

질문 # 253
......

CDPSE퍼펙트 덤프데모 다운로드: https://www.dumptop.com/ISACA/CDPSE-dump.html

그리고 DumpTOP CDPSE 시험 문제집의 전체 버전을 클라우드 저장소에서 다운로드할 수 있습니다: https://drive.google.com/open?id=1VkZgu0jVhL_upec1qhOp3ubl8rfc5x-m