CIPT$^{\text{Q\&As}}$

Certified Information Privacy Technologist (CIPT)

Pass IAPP CIPT Exam with 100% Guarantee

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

https://www.leads4pass.com/cipt.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

How can a hacker gain control of a smartphone to perform remote audio and video surveillance?

A. By performing cross-site scripting.

B. By installing a roving bug on the phone.

C. By manipulating geographic information systems.

D. By accessing a phone\\'s global positioning system satellite signal.

Correct Answer: B

QUESTION 2

A user who owns a resource wants to give other individuals access to the resource. What control would apply?

A. Mandatory access control.

B. Role-based access controls.

C. Discretionary access control.

D. Context of authority controls.

Correct Answer: B

Reference: https://docs.microsoft.com/bs-latn-ba/azure/role-based-access-control/overview

QUESTION 3

Which is NOT a suitable action to apply to data when the retention period ends?

A. Aggregation.

B. De-identification.

C. Deletion.

D. Retagging.

Correct Answer: D

Retagging is not a suitable action to apply to data when the retention period ends2 . Retagging means changing the classification or label of data based on its sensitivity or value2. Retagging does not reduce the risk of unauthorized access or disclosure of personal data that is no longer needed by the organization2. The other options are suitable actions to apply to data when the retention period ends, as they either remove or anonymize personal data2.

QUESTION 4

Which of the following is considered a client-side IT risk?

A. Security policies focus solely on internal corporate obligations.

B. An organization increases the number of applications on its server.

C. An employee stores his personal information on his company laptop.

D. IDs used to avoid the use of personal data map to personal data in another database.

Correct Answer: C

An employee stores his personal information on his company laptop. This is considered a client-side IT risk because it involves the actions of an employee who has control over the use of their individual device. Client-side IT risk refers to the potential threats that arise from devices or applications that are used by end-users or customers3. An employee storing his personal information on his company laptop is an example of client-side IT risk, as it exposes sensitive data to unauthorized access, theft or loss. The other options are examples of server-side IT risk, which involves threats that originate from systems or networks that host applications or services3.

QUESTION 5

Which of the following became a foundation for privacy principles and practices of countries and organizations across the globe?

A. The Personal Data Ordinance.

B. The EU Data Protection Directive.

C. The Code of Fair Information Practices.

D. The Organization for Economic Co-operation and Development (OECD) Privacy Principles.

Correct Answer: D

Reference: https://privacyrights.org/resources/review-fair-information-principles-foundation- privacy-public-policy

The Organization for Economic Co-operation and Development (OECD) Privacy Principles became a foundation for privacy principles and practices of countries and organizations across the globe4. The OECD Privacy Principles were adopted by OECD member countries in 1980 as a set of eight basic principles for ensuring adequate protection of personal data across national borders4. The OECD Privacy Principles have been widely recognized as an international standard for data protection and have influenced many regional and national laws and frameworks4.

QUESTION 6

Which of the following most embodies the principle of Data Protection by Default?

A. A messaging app for high school students that uses HTTPS to communicate with the server.

B. An electronic teddy bear with built-in voice recognition that only responds to its owner\\'s voice.

C. An internet forum for victims of domestic violence that allows anonymous posts without registration.

D. A website that has an opt-in form for marketing emails when registering to download a whitepaper.

Correct Answer: D

QUESTION 7

An organization must terminate their cloud vendor agreement immediately. What is the most secure way to delete the encrypted data stored in the cloud?

A. Transfer the data to another location.

B. Invoke the appropriate deletion clause in the cloud terms and conditions.

C. Obtain a destruction certificate from the cloud vendor.

D. Destroy all encryption keys associated with the data.

Correct Answer: D

Destroying all encryption keys associated with encrypted data stored on a cloud server would make that encrypted data inaccessible even if it still exists on that server 4.

QUESTION 8

Which of the following modes of interaction often target both people who personally know and are strangers to the attacker?

A. Spam.

B. Phishing.

C. Unsolicited sexual imagery.

D. Consensually-shared sexual imagery.

Correct Answer: B

QUESTION 9

What would be an example of an organization transferring the risks associated with a data breach?

A. Using a third-party service to process credit card transactions.

B. Encrypting sensitive personal data during collection and storage

C. Purchasing insurance to cover the organization in case of a breach.

D. Applying industry standard data handling practices to the organization\\' practices.

Correct Answer: C

Reference: http://www.hpso.com/Documents/pdfs/newsletters/firm09-rehabv1.pdf

Purchasing insurance to cover the organization in case of a breach. By purchasing insurance, the organization can transfer the financial risks associated with a data breach to an insurance provider. This is a risk management strategy that can help an organization mitigate the financial impact of a breach.

Transferring risk means shifting some or all of the potential losses or liabilities associated with a risk to another party2. Purchasing insurance is one way of transferring risk, as it allows the organization to share the financial burden of a data breach with an insurer. The other options do not involve transferring risk, but rather reducing, avoiding or accepting it.

QUESTION 10

A BaaS provider backs up the corporate data and stores it in an outsider provider under contract with the organization. A researcher notifies the organization that he found unsecured data in the cloud. The organization looked into the issue and realized $ne of its backups was misconfigured on the outside provider\\'s cloud and the data fully exposed to the open internet. They quickly secured the backup. Which is the best next step the organization should take?

A. Review the content of the data exposed.

B. Review its contract with the outside provider.

C. Investigate how the researcher discovered the unsecured data.

D. Investigate using alternate BaaS providers or on-premise backup systems.

Correct Answer: B

The best next step the organization should take is to review its contract with the outside provider. This will help the organization to identify the responsibilities of the outside provider and the organization in the event of a data breach.

QUESTION 11

A privacy technologist has been asked to aid in a forensic investigation on the darknet following the compromise of a company\\'s personal data. This will primarily involve an understanding of which of the following privacy-preserving techniques?

A. Encryption

B. Do Not Track

C. Masking

D. Tokenization

Correct Answer: A

a privacy technologist aiding in a forensic investigation on the darknet following the compromise of a company\\'s personal data would primarily need an understanding of encryption. Encryption is a privacy-preserving technique that can help protect sensitive data from unauthorized access.

QUESTION 12

Which is the most accurate type of biometrics?

A. DNA

B. Voiceprint.

C. Fingerprint.

D. Facial recognition.

Correct Answer: B

Reference: https://www.bayometric.com/biometrics-face-finger-iris-palm-voice/

QUESTION 13

You are a wine collector who uses the web to do research about your hobby. You navigate to a news site and an ad for wine pops up. What kind of advertising is this?

A. Remnant.

B. Behavioral.

C. Contextual.

D. Demographic.

Correct Answer: B

Reference: https://neilpatel.com/blog/behavioral-advertising/

QUESTION 14

Which of the following is the least effective privacy preserving practice in the Systems Development Life Cycle (SDLC)?

A. Conducting privacy threat modeling for the use-case.

B. Following secure and privacy coding standards in the development.

C. Developing data flow modeling to identify sources and destinations of sensitive data.

D. Reviewing the code against Open Web Application Security Project (OWASP) Top 10 Security Risks.

Correct Answer: C

QUESTION 15

An organization\\'s customers have suffered a number of data breaches through successful social engineering attacks. One potential solution to remediate and prevent future occurrences would be to implement which of the following?

A. Differential identifiability.

B. Multi-factor authentication.

C. Greater password complexity.

D. Attribute-based access control.

Correct Answer: B

Multi-factor authentication. Social engineering attacks often involve tricking individuals into revealing their login credentials. Implementing multi-factor authentication can help prevent unauthorized access even if an attacker obtains a user\\'s password.