DUMPSARENA

QPA_NQualified PIN Assessor (QPA New)

PCI SSC qpa_n

Version Demo

Total Demo Questions: 10

Total Premium Questions: 107

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which of the following are important for securing wireless networks that handle cardholder data?

A. Using WPA2 or stronger encryption

B. Disabling SSID broadcasting

C. Changing default passwords and settings

D. Conducting regular wireless scans

E. Using firewalls to segregate wireless networks

ANSWER: A C D E

Explanation:

Securing wireless networks involves using WPA2 or stronger encryption, changing default passwords, conducting regular wireless scans, and using firewalls to segregate wireless networks. Disabling SSID broadcasting is not a PCI DSS requirement but can enhance security. PCI DSS Wireless Guidelines

QUESTION NO: 2

What measures should be taken to secure wireless networks that transmit cardholder data?

A. Disabling SSID broadcasting

B. Using WPA2 or stronger encryption

C. Changing default wireless settings

D. Implementing wireless intrusion detection/prevention

E. Using open wireless networks for convenience

ANSWER: B C D

Explanation:

Securing wireless networks involves using WPA2 or stronger encryption, changing default wireless settings, and implementing wireless intrusion detection/prevention. Disabling SSID broadcasting and using open wireless networks are not secure practices. PCI DSS Wireless Guidelines

QUESTION NO: 3

Which of the following are required actions for logging and monitoring access to cardholder data?

A. Logging all access attempts, including failures

B. Encrypting log files

C. Reviewing logs at least daily

D. Retaining logs for a minimum of one year

E. Allowing modification of logs by administrators

ANSWER: A B D

Explanation:

Required actions for logging and monitoring access to cardholder data include logging all access attempts, encrypting log files, and retaining logs for at least one year. Logs should be reviewed at least daily. Allowing modification of logs is not recommended. PCI DSS Requirement 10

QUESTION NO: 4

Which of the following practices are required for protecting cardholder data during transmission?

A. Using strong cryptographic protocols

B. Implementing secure sockets layer (SSL)

C. Using Transport Layer Security (TLS)

D. Encrypting data at the application layer

E. Restricting access to transmission logs

ANSWER: A C D E

Explanation:

Protecting cardholder data during transmission requires using strong cryptographic protocols, Transport Layer Security (TLS), encrypting data at the application layer, and restricting access to transmission logs. SSL is deprecated and should not be used. PCI DSS Requirement 4

QUESTION NO: 5

Which of the following practices are necessary for maintaining a secure software development lifecycle (SDLC)?

A. Defining security requirements at the outset

B. Performing regular security testing

C. Storing source code in a public repository

D. Conducting security training for developers

E. Documenting security defects and their resolution

ANSWER: A B D E

Explanation:

Maintaining a secure SDLC involves defining security requirements at the outset, performing regular security testing, conducting security training for developers, and documenting security defects and their resolution. Storing source code in a public repository is not secure. PCI DSS Requirement 6

QUESTION NO: 6

Which of the following are considered valid authentication methods according to PCI DSS?

A. Passwords

B. Biometrics

C. Single-factor authentication

D. Multi-factor authentication

E. PINs

ANSWER: A B D E

Explanation:

Valid authentication methods include passwords, biometrics, multi-factor authentication, and PINs. Single-factor authentication alone is not sufficient. PCI DSS Requirement 8

QUESTION NO: 7

Which of the following measures are necessary for protecting cardholder data during transmission over open, public networks?

A. Using strong cryptographic protocols such as TLS

B. Encrypting data at the application layer

C. Implementing secure sockets layer (SSL)

D. Regularly updating encryption algorithms

E. Transmitting PAN in plaintext emails

ANSWER: A B D E

Explanation:

Protecting cardholder data during transmission involves using strong cryptographic protocols such as TLS, encrypting data at the application layer, implementing SSL (or preferably TLS), and regularly updating encryption algorithms. Transmitting PAN in plaintext emails is not secure. PCI DSS Requirement 4

QUESTION NO: 8

Which of the following are necessary for maintaining secure wireless networks?

A. Using WPA2 or stronger encryption

B. Changing default SSID and passwords

C. Disabling wireless security

D. Conducting regular wireless scans

E. Using wireless access points with built-in firewalls

ANSWER: A B D E

Explanation:

Maintaining secure wireless networks involves using WPA2 or stronger encryption, changing default SSID and passwords, conducting regular wireless scans, and using wireless access points with built-in firewalls. Disabling wireless security is not recommended. PCI DSS Wireless Guidelines

QUESTION NO: 9

Which of the following are practices for managing and controlling physical access to cardholder data?

A. Use of surveillance cameras

B. Limiting access to authorized personnel only

C. Regularly changing physical locks

D. Unrestricted access to all employees

E. Monitoring and logging physical access

ANSWER: A B C E

Explanation:

Managing physical access involves using surveillance cameras, limiting access to authorized personnel, regularly changing locks, and monitoring and logging access. Unrestricted access is not recommended. PCI DSS Requirement 9

QUESTION NO: 10

Which of the following are necessary for maintaining secure system configurations?

A. Regularly updating system configurations

B. Using default vendor settings

C. Conducting configuration audits

D. Disabling unnecessary services

E. Allowing unrestricted user access

ANSWER: A C D

Explanation:

Maintaining secure system configurations requires regularly updating configurations, conducting audits, and disabling unnecessary services. Using default vendor settings and allowing unrestricted user access are not secure practices. PCI DSS Requirement 2