2/26 **2111E755** Candidate's Seat No :________

M.Sc Sem-3 Examination

502

Cyber Security & Forensic (EB) ISMS-PCI

Time : 2-30 Hours] **November-2024** **[Max. Marks : 70**

Question 1 Answer the following questions:

i. What are the levels of merchants and service providers? What is the significance of the different levels? 7Marks

ii. Explain the steps involved in implementing a firewall configuration that complies with PCI DSS requirements 7Marks

OR

i. What is a Statement of applicability? Explain benefits of SOA in ISMS. 7Marks

ii. Describe the process an organization should follow to identify and change vendor-supplied default passwords and configurations. What tools or methods can assist in this process? 7Marks

Question 2 Answer the following questions:

i. What essential features should an effective anti-virus solution possess for PCI DSS compliance, and what functionalities enhance malware protection? Additionally, explain the importance of regular malware scans, including recommended frequencies and influencing factors. 7Marks

ii. Why is encryption essential for transmitting cardholder data across open, public networks? Discuss the potential risks of transmitting unencrypted data. Mention the steps organizations should take to ensure secure transmission of cardholder data. 7Marks

OR

i. Illustrate common secure coding techniques and describe the role of secure coding practices in the development of applications that handle cardholder data. What measures should organizations implement to ensure that third-party applications are secure and comply with PCI DSS requirements? 7Marks

ii. What are the reasons for protecting stored cardholder data? Additionally, explain the process for regularly testing security systems and processes to protect the data with specific testing methods that should be employed. 7Marks

Question 3 Answer the following questions:

i. What are the key components of a penetration testing report? Discuss the role of internal and external penetration testing. How do these tests differ, and what specific objectives should each type of aim to achieve? 7Marks

ii. How should organizations ensure that access is appropriately granted and revoked? Explain the role of logging and monitoring in identifying and authenticating áccess to system components. What specific events should be logged to comply with PCI DSS? 7Marks

OR

i. How can organizations respond to suspicious activity detected through access monitoring? Outline the steps involved in an incident response plan specific to unauthorized access attempts. Explain the importance of real-time monitoring of access to network resources. 7Marks

(P.T.O)

E 755-2

ii. Discuss the significance of maintaining a physical security policy. What key elements should be included in this policy to ensure compliance with PCI DSS? 7Marks

What processes should be in place for securely disposing of physical media that contair cardholder data?

Questions 4 Answer the following questions:

i. What are the primary objectives of a PCI DSS audit, how do they enhance the security of cardholder data, and what preparation steps, including necessary documentation, should organizations take before the audit? 7Marks

ii. Discuss the importance of fostering a culture of security within the organization to support continuous improvement in PCI DSS compliance. What strategies can leadership implement to promote this culture among employees? 7Marks

OR

i. Describe the importance of enforcing the information security policy within the organization. What disciplinary measures should be established for non-compliance with the policy? 7Marks

ii. Discuss the role of senior management in the success of an information security policy. How can leadership promote a culture of security within the organization? 7Marks

Questions 5 Attempt any Seven out of Twelve. 14Marks

1. Give at least two differences between information security and cybersecurity.
2. Define following:

   a. SAQs b. RoC c. AoC
3. What are the objectives of PCI DSS?
4. How can organizations ensure that only authorized personnel have access to firewall configurations?
5. Explain steps of card payment.
6. How can organizations leverage technology to enhance their PCI DSS compliance efforts?
7. What strategies should be involved for senior leadership effectively?
8. What tools and techniques can organizations use to achieve effective real-time monitoring?
9. What does the principle of "least privilege" mean in the context of PCI DSS.
10. What training and awareness programs should organizations implement to educate employees about malware threats and the importance of anti-virus measures?
11. Which of the following is NOT one of the 12 PCI-DSS requirements?

    A. Install and maintain a firewall configuration to protect cardholder data

    B. Regularly update anti-virus software or programs

    C. Avoid encrypting transmission of cardholder data

    D. Restrict access to cardholder data by business need to know
12. Which of the following correctly describes a PCI-DSS Qualified Security Assessor (QSA)?

    A. A professional certified to perform PCI-DSS audits

    B. A payment processor

    C. An organization that issues credit cards

    D. A third-party vendor for card storage

....X..X..