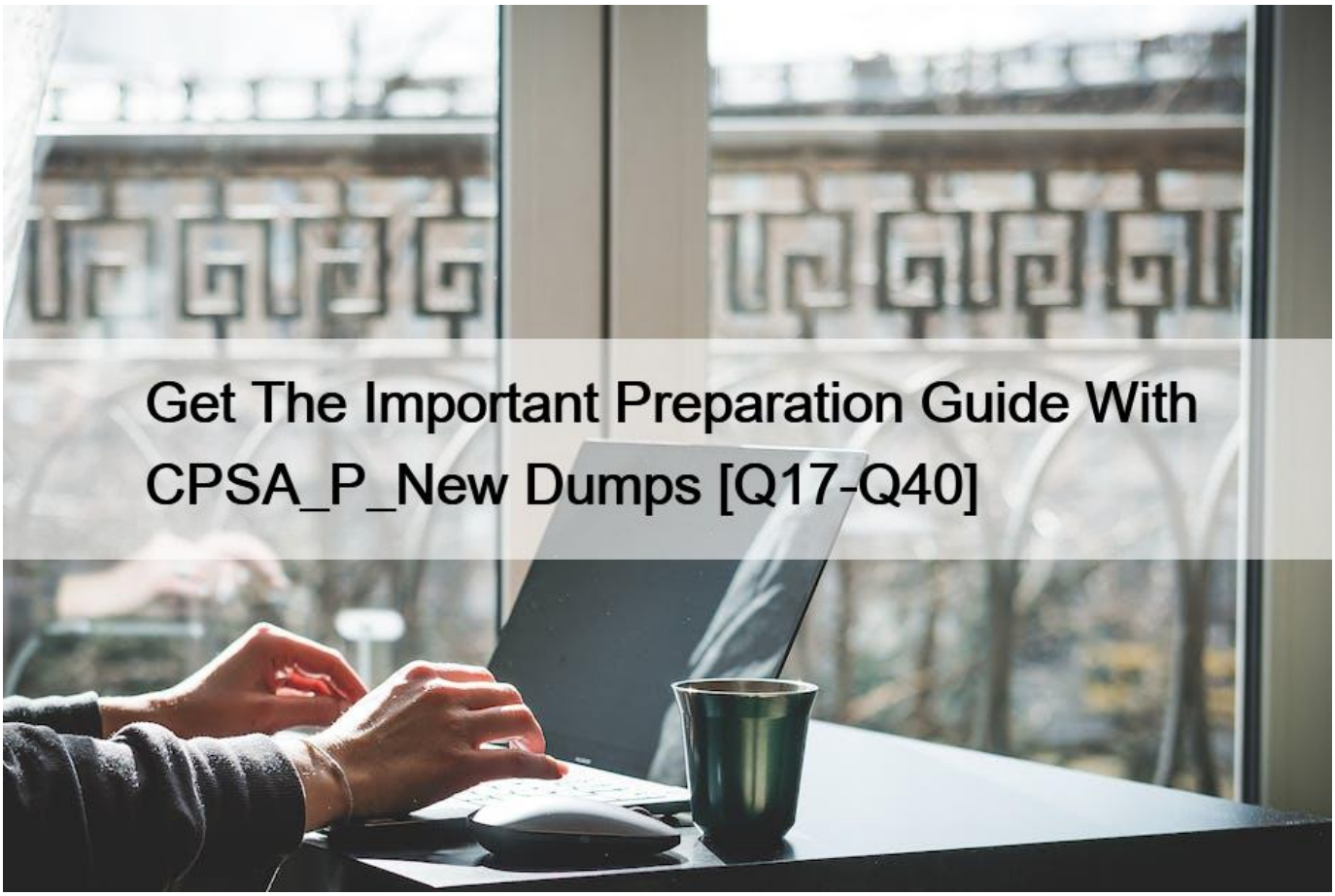
# Get The Important Preparation Guide With CPSA_P_New Dumps [Q17-Q40




**Get The Important Preparation Guide With CPSA_P_New Dumps Get Totally Free Updates on CPSA_P_New Dumps PDF Questions NEW QUESTION 17**

A card production vendor employs a contracted guard service from an outside source. What is one of the responsibilities of the contracted service?

* Provide only certified guards
* Register their service with the VPA
* Maintain their own liability insurance in case of losses to card material
* Undergo their own Card Production assessment and provide evidence of a passing result

Explanation

According to the PCI Card Production Physical Security Requirements, one of the security controls for contracted guard services is to ensure that they maintain their own liability insurance in case of losses to card material. This is to protect the card production vendor from any financial losses or damages caused by the contracted guard service, such as negligence,theft, or misuse of card material. The contracted guard service should also comply with the vendor’s security policies and procedures, and undergo background checks and security training. References: PCI Card Production Physical Security Requirements, Version 1.0, April 2019, Section 1.1, Objective 2, Requirement 2.2.1, Page 71

**NEW QUESTION 18**

In which of the following locations must the CCTV and access control servers be located?
* Within the secure server room inside of the HSA
* Within the Security Control Room (SCR)
* Within a room in the HSA with security controls equivalent to the SCR applied
* Within the SCR or a room with equivalent security
Explanation

According to the PCI Card Production Physical Security Requirements, the CCTV and access control servers must be located within the Security Control Room (SCR) or a room with equivalent security. This means that the room must have the same level of physical protection as the SCR, such as locks, alarms, sensors, cameras, and access control devices. The purpose of this requirement is to prevent unauthorized access, tampering, or theft of the servers that store and process sensitive data related to card production and security. References: PCI Card Production Physical Security Requirements, v2.0, April 2019, page 16

**NEW QUESTION 19**

Who performs regular AQM audits of CPSA companies?
* Issuing banks
* Payment brands
* PCI SSC
* Vendor
Explanation

The PCI Security Standards Council (PCI SSC) performs regular Assessor Quality Management (AQM) audits of CPSA companies to ensure that they comply with the PCI CPSA Qualification Requirements and the PCI Card Production Standards. The AQM audits are conducted by PCI SSC staff or authorized third parties, and may include onsite visits, remote reviews, or both. The AQM audits aim to verify the quality and consistency of the CPSA companies’ assessment processes, reports, and documentation, as well as their adherence to the PCI SSC Code of Professional Responsibility. The AQM audits may result in corrective actions, sanctions, or revocation of the CPSA company status, depending on the severity and frequency of the non-compliance issues identified. References:

PCI Card Production Security Assessor (CPSA) Qualification Requirements, v1.0, April 2019, page 12, requirement 8.1 PCI Card Production Security Assessor (CPSA) Program Guide, v1.0, April 2019, page 6, section 3.2

**NEW QUESTION 20**

A vendor’s HSA access is enforced by a security turnstile they have a logical access-control system that ensures anti pass-back. The device is functioning correctly. When must the status of the access change?
* Only when an unauthorised badge is presented
* Only when the person has successfully completed the access cycle
* Upon initial entry of the person into the device, prior to completion of the access cycle
* Upon initial presentation of an authorised badge, prior to completion of the access cycle
Explanation

According to the PCI Card Production Logical Security Requirements, a vendor’s HSA access must be enforced by a security turnstile that has a logical access-control system that ensures anti pass-back. This means that the system must prevent a person from using the same badge to enter or exit the HSA more than once without completing the access cycle. The access cycle is the process of entering or exiting the HSA through the turnstile, which may involve biometric verification, PIN entry, or other authentication methods. The status of the access must change upon initial presentation of an authorised badge, prior to completion of

the access cycle, to prevent another person from using the same badge to enter or exit the HSA. For example, if a person presents an authorised badge to enter the HSA, the system must register that the badge is inside the HSA and deny access to anyone else who tries to use the same badge until the person exits the HSA with the same badge. References: PCI Card Production Logical Security Requirements, v2.0, April 2019, page 12

**NEW QUESTION 21**

Who is required to approve visitor entry to the HSA or cloud-based provisioning environment?
* The head of the vendor facility
* The Security Manager
* Both the Security Manager and the Production Manager
* The Security Manager, Production Manager, and the head of the vendor facility
Explanation

According to the PCI Card Production and Provisioning – Physical Security Requirements, the Security Manager is the person who is responsible for approving visitor entry to the High Security Area (HSA) or cloud-based provisioning environment. The HSA is the area where card production and provisioning activities take place, such as card manufacturing, personalization, PIN generation and printing, and fulfillment. The cloud-based provisioning environment is the logical equivalent of the HSA for entities that provide over-the-air (OTA) provisioning or host card emulation (HCE) provisioning services. The Security Manager must ensure that visitors have a legitimate business need toenter the HSA or cloud-based provisioning environment, and must authorize their access in advance. The Security Manager must also maintain a visitor log that records the visitor’s name, company, date, time, and purpose of visit, as well as the escort’s name and signature. The Security Manager must also ensure that visitors are escorted by authorized personnel at all times, and that they wear a distinctive visitor badge. The head of the vendor facility, the Production Manager, or any other person is not required to approve visitor entry to the HSA or cloud-based provisioning environment, unless they are also designated as the Security Manager by the vendor. References:

Payment Card Industry (PCI) Card Production and Provisioning – Physical Security Requirements, Section 3.1.1 and 3.1.2
Payment Card Industry (PCI) Card Production and Provisioning – Glossary of Terms, Abbreviations, and Acronyms, Definitions of Security Manager, High Security Area, Cloud-Based Provisioning Environment, OTA Provisioning, and HCE Provisioning

**NEW QUESTION 22**

Which of the follow best describes a Technical FAQ?
* Technical FAQs only apply to the specific technology as the FAQ defines it
* Technical FAQs can be submitted to PCI SSC at any time
* Use of the Technical FAQs is mandatory, they shall be used during an assessment
* Use of the Technical FAQs is optional, they are considered guidance
Explanation

According to the PCI CPSA Qualification Requirements, Technical FAQs are documents that provide guidance on specific technical topics related to the PCI Card Production Security Standards. Technical FAQs are not mandatory, but they are recommended to be used by CPSA Companies and CPSA Employees during the card production assessment process. Technical FAQs are intended to help clarify the intent and applicability of the PCI Card Production Security Requirements, and to provide examples and best practices for achieving compliance. Technical FAQs are published by the PCI SSC on its website, and are updated periodically based on feedback from the card production industry and the payment brands. References: PCI CPSA Qualification Requirements, Version 1.1, April 2020, Section 4.2, Page 81

**NEW QUESTION 23**

The vendor’s technical documentation shows that the alarm system does not send alerts to the security control room. After a discussion you learn that the alarm works perfectly, and sends a clear signal to summon the local police every time an emergency exit is opened. Why might this cause a problem for their assessment?
* If the local police have not been issued with an exterior key. they will not be able to investigate the cause of the alarm and reset it
* During working hours, the alarm should be managed in the security control room, or by a central monitoring service
* If the local police receive too many false-positive alerts, they may not respond within 15 minutes of the alarm
* During busy times, the local police may not be able to respond

Explanation

According to the PCI Card Production and Provisioning Physical Security Requirements, the vendor must have an alarm system that monitors and detects unauthorized access to the card production and provisioning facilities, and that alerts the security control room or a central monitoring service. The alarm system must also be able to identify the location and cause of the alarm, and allow authorized personnel to reset it. The alarm system must be operational 24/7, and must be tested at least annually. The vendor must also have procedures to respond to alarms and incidents, and to report them to the relevant parties. If the alarm system does not send alerts to the security control room, or a central monitoring service, during working hours, the vendor may not be able to comply with these requirements, and may not be able to prevent, detect, or respond to unauthorized access or security breaches. This may cause a problem for their assessment, as they may not meet the PCI Card Production and Provisioning Physical Security Requirements. References: PCI Card Production and Provisioning Physical Security Requirements and Test Procedures v3.0, January 2022, pages 9-101

**NEW QUESTION 24**

During an assessment you ask to see employee records for employees with access to the HSA. The records include information about the screening process, including background information from the employee application process. The oldest background Information that is available is for an employee that left the vendor (terminated their contract) one year previously. You note this as non-compliant, why?
* Employee information, including background checks, must be stored for at least seven years
* Employee information must be securely destroyed (e.g. securely wiped) within 2 years (after termination of contract)
* The vendor must retain the background information for at least 18 months after termination of contract
* The vendor must only retain background information for all current employees, not for those that have been terminated

Explanation

According to the PCI Card Production Logical Security Requirements, the vendor must securely destroy all employee information, including background checks, within two years of the employee’s termination of contract. This is to prevent unauthorized access to sensitive employee data and to comply with the PCI DSS requirement 3.1, which states that cardholder data must not be stored longer than necessary. The vendor must also have a documented policy and procedure for the secure destruction of employee information, and must maintain a log of all destruction activities. References:

PCI Card Production Logical Security Requirements, v2.0, April 2019, page 19, requirement 6.1.1 PCI DSS, v3.2.1, May 2018, page 25, requirement 3.1

**NEW QUESTION 25**

Which of the following must every assessor do to maintain their CPSA certification?
* Complete annual requalification training or complete 3 assessments for different facilities each year
* Earn and document at least 20 hours of Continuing Professional Education (CPE) over 3 years
* Earn an additional professional certification from List A or B of the Qualification Requirements (QRs)
* Submit evidence of internal training in a relevant area (as per the QRs)

Explanation

According to the Card Production Security Assessor (CPSA) Qualification Requirements, CPSAs must maintain their qualification status by either completing the annual requalification training provided by PCI SSC or performing at least three (3) PCI Card Production Assessments for different facilities over the previous one-year period. This ensures that CPSAs remain current with technical and industry changes and demonstrate professionalism. References: Card Production Security Assessor (CPSA) Qualification Requirements, v1.1, March 2022, page 10

**NEW QUESTION 26**

A vendor discovers that a recent shipment of cards is missing a set. Which of the following responses would you expect in a compliant organization?
* An immediate call is made to the issuer and the VPA who, between them, contact law enforcement and put together a joint statement
* The head of security initiates a meeting, and once the VPA approves the messaging, law enforcement is notified in two days
* A report is requested by the issuer, the vendor sends it to them, and the issuer handles the incident with the local police
* After an incident review, the VPA, issuer and law enforcement are all notified within 24 hours
Explanation

According to the PCI Card Production Physical Security Requirements, one of the security controls for card shipment is to ensure that the vendor has an incident response plan in place to handle any card shipment incidents, such as loss, theft, or tampering. The incident response plan should include the following steps1:

The vendor should conduct an incident review to determine the cause and scope of the incident, and document the findings and actions taken.

The vendor should notify the VPA, the issuer, and law enforcement of the incident within 24 hours of discovery, or as soon as possible.

The vendor should cooperate with the VPA, the issuer, and law enforcement in the investigation and resolution of the incident, and provide any evidence or information requested.

The vendor should implement corrective actions to prevent the recurrence of the incident, and report the results to the VPA and the issuer. Therefore, the response that best reflects a compliant organization is option D, which follows the steps of the incident response plan as required by the PCI Card Production Physical Security Requirements. References: PCI Card Production Physical Security Requirements, Version 1.0, April 2019, Section 1.1, Objective 6, Requirement 6.2, Page 131

**NEW QUESTION 27**

An assessor must provide which of the following to their client at the start of every assessment?
* CPSA Feedback Form
* Quality Assurance Manual
* Attestation of Compliance
* Vendor Release Agreement
Explanation

According to the Card Production Security Assessor (CPSA) Qualification Requirements, an assessor must provide their client with a Quality Assurance Manual at the start of every assessment. The Quality Assurance Manual is a document that describes the assessor’s methodology, procedures, and quality control measures for conducting assessments. The manual must be consistent with the CPSA Program Guide and the PCI Card Production and Provisioning Security Requirements. The manual must also include a description of the assessor’s roles and responsibilities, the assessment scope and objectives, the assessment plan and timeline, the assessment report format and content, and the assessor’s conflict of interestpolicy. References: Card

Production Security Assessor (CPSA) Qualification Requirements, v1.0, April 2019, page 111

**NEW QUESTION 28**

For how long must a vendor retain all applicant and employee background information on file?
* For at least 12 months after termination of the contract of employment
* For at least 18 months after termination of the contract of employment
* For at least 24 months after termination of the contract of employment
* It is not a requirement to store this information beyond termination of the contract
Explanation

According to the PCI CPSA Qualification Requirements, one of the administrative requirements for CPSA Companies is to retain all applicant and employee background information on file for at least 12 months after termination of the contract of employment. This is to ensure that the CPSA Company can provide evidence of the background checks performed on the CPSA Employees or other personnel involved in card production and provisioning activities. The background checks should include criminal history, employment history, education verification, and reference checks, and should be conducted at least every two years or upon rehire. References: PCI CPSA Qualification Requirements, Version 1.1, April 2020, Section 6.1.2, Page 111

**NEW QUESTION 29**

Which of the following security awareness measures is required for compliance?
* Annual training on common attack methods
* Annual training on use of mantraps
* Security awareness exams for all personnel
* Security posters must be placed in the facility
Explanation

According to the PCI Card Production and Provisioning Logical Security Requirements, the vendor must implement a formal security awareness program to make all personnel aware of the importance of card production and provisioning security. The security awareness program must include annual training on common attack methods, such as phishing, social engineering, malware, and ransomware, and how to prevent, detect, and report them. The security awareness program must also include training on the vendor’s security policies and procedures, the roles and responsibilities of personnel, the applicable PCI Card Production and Provisioning Security Requirements, and the consequences of non-compliance. The vendor must also require all personnel to acknowledge at least annually that they have read and understood the security policies and procedures. The vendor must not use security posters alone, as they are not sufficient to meet the security awareness program requirements. The vendor may use security awareness exams for all personnel, but they are not mandatory for compliance. The vendor may also train personnel on the use of mantraps, but this is not relevant to the logical security requirements. References: PCI Card Production and Provisioning Logical Security Requirements and Test Procedures v3.0, January 2022, pages 28-291

**NEW QUESTION 30**

For how long must a CPSA Company maintain workpapers and technical information obtained during an assessment?
* Until each applicable payment brand has accepted (and signed off) the ROC and AOC
* As long as the entity under assessment is a client of the CPSA Company
* 3 years
* 1 year
Explanation

According to the PCI CPSA Program Guide, a CPSA Company must maintain workpapers and technical information obtained during an assessment for a minimum of three years from the date of the assessment. The workpapers and technical information must

be stored securely and made available to PCI SSC upon request.

The workpapers and technical information must include, but are not limited to, the following:

The Card Production Report on Compliance (ROC) and the Card Production Attestation of Compliance (AOC) The Card Production Entity’s policies and procedures The Card Production Entity’s network diagrams and data flow diagrams The results of any testing performed by the CPSA Company or the Card Production Entity The evidence of any remediation actions taken by the Card Production Entity The correspondence between the CPSA Company and the Card Production Entity The correspondence between the CPSA Company and the payment brands The feedback form completed by the Card Production Entity References:

PCI Card Production Security Assessor (CPSA) Program Guide, Version 1.0, April 2019, page 111

**NEW QUESTION 31**

When must HSA motion detectors generate an alarm event?
* Each time movement is detected
* Each time movement is detected outside of regular business hours
* Each time movement is detected and the access-control system indicates the room is occupied
* Each time movement is detected and the access-control system indicates the room is not occupied

Explanation

According to the PCI Card Production Physical Security Requirements, one of the security controls for high-security areas (HSAs) is to have motion detectors that generate an alarm event when movement is detected and the access-control system indicates the room is not occupied. This is to prevent unauthorized access or intrusion to the HSAs, where sensitive card production and provisioning activities take place. The motion detectors should be configured to cover all areas within the HSA and should be tested periodically to ensure proper functionality. References: PCI Card Production Physical Security Requirements, Version 1.0, April 2019, Section 1.1, Objective 2, Requirement 2.1.1, Page 61

**NEW QUESTION 32**

A vendor puts cardholder information into a chip by sliding a payment card through a machine that programs it and verifies the data. The chip can make contactless transactions. Which of the following best describes the vendor’s activity?
* Card personalization
* Host Card Emulation (HCE) provisioning
* Secure Element (SE) provisioning
* Fulfillment

Explanation

Card personalization is the process of transferring cardholder information, such as account number, name, expiration date, and other data, to a payment card. This can be done by various methods, such as magnetic stripe encoding, embossing, laser engraving, or chip programming. Chip programming is the method of personalizing a card that has an embedded microchip that can store and process data. Chip cards can support contact or contactless transactions, depending on the chip type and the terminal capabilities. Contact transactions require the card to be inserted into a reader, while contactless transactions use radio frequency (RF) communication between the card and the reader. The vendor in the question is performing card personalization by programming the chip and verifying the data on the card. References:

Payment Card Industry (PCI) Card Production and Provisioning – Logical Security Requirements, Section 1.1.1 Payment Card Industry (PCI) Card Production and Provisioning – Physical Security Requirements, Section 1.1.1 Payment Card Industry (PCI) Card Production and Provisioning – Glossary of Terms, Abbreviations, and Acronyms, Definitions of Card Personalization, Chip Card, Contact Card, and Contactless Card

**NEW QUESTION 33**

A cardholder wants to make purchases using their phone, so they have their cardholder information programmed into their SIM card using their mobile phone provider. Which of the following best describes this system?
* Card personalization
* Host Card Emulation (HCE) provisioning
* Secure Element (SE) provisioning
* Over-the-air (OTA) provisioning

Explanation

According to the PCI Card Production and Provisioning Logical Security Requirements, Secure Element (SE) provisioning is the process of adding cardholder account information to a secure element on a mobile device via an over-the-air or over-the-internet communication channel. A secure element is a tamper-resistant platform that can securely host applications and their confidential and cryptographic data. A SIM card is an example of a secure element that can be used for mobile payments. SE provisioning is different from Host Card Emulation (HCE) provisioning, which is the process of adding cardholder account information to a cloud-based server that emulates a secure element on a mobile device. SE provisioning is also different from card personalization, which is the process of adding cardholder account information to a physical card.

Over-the-air (OTA) provisioning is a generic term that can refer to either SE or HCE provisioning, depending on the type of mobile payment system used. References: PCI Card Production and Provisioning Logical Security Requirements and Test Procedures v3.0, January 2022, pages 6-71

**NEW QUESTION 34**

John works for ACME Inc Personalizers. an organization that personalizes payment cards as well as printing the corresponding PIN mailers for distribution directly to the cardholder. Which of the following statements is true?
* If John is involved in card personalization then he must not be involved in the printing of the corresponding PINs
* If John is involved in card personalization, then he must never be involved in the card shipment process
* If John is involved in card personalization, then he must never be involved in PIN printing
* If John is involved in PIN printing, then he must never be involved in the card shipment process

Explanation

According to the PCI Card Production and Provisioning – Logical Security Requirements, there must be a clear segregation of duties between the staff involved in different card production and provisioning activities, such as card personalization, PIN generation and printing, and card fulfillment. This is to prevent any unauthorized access, modification, or disclosure of sensitive cardholder data and to ensure the integrity and confidentiality of the card production process. Therefore, if John is involved in card personalization, which is the process of transferring cardholder information to a payment card, then he must never be involved in PIN printing, which is the process of printing the personal identification number associated with the cardholder account on a mailer. This way, John cannot link the cardholder data on the card with the PIN on the mailer, and cannot compromise the security of the cardholder authentication. The other statements are not true, as there is no requirement that prohibits John from being involved in the card shipment process, as long as he does not have access to both the card and the PIN mailer at the same time. References:

Payment Card Industry (PCI) Card Production and Provisioning – Logical Security Requirements, Section 2.1.1 and 2.1.2
Payment Card Industry (PCI) Card Production and Provisioning – Glossary of Terms, Abbreviations, and Acronyms, Definitions of Card Personalization and PIN Printing

**NEW QUESTION 35**

A vendor is unsure which forms are needed to complete an assessment. Who should they ask?

* Assessor
* Issuing banks
* Payment brands
* PCI SSC

Explanation

The assessor is the person who conducts the PCI Card Production Security Assessment and prepares the Card Production Report on Compliance (ROC) and the Card Production Attestation of Compliance (AOC). The assessor should be familiar with the forms that are needed to complete an assessment and provide guidance to the vendor on how to fill them out. The assessor should also ensure that the forms are consistent with the PCI Card Production Standards and the PCI CPSA Qualification Requirements. The other options are not the best sources of information for the vendor, as they may not be directly involved in the assessment process or have the expertise to advise on the forms. References:

PCI Card Production Security Assessor (CPSA) Program Guide, Version 1.0, April 2019, page 81 PCI Card Production Security Assessor (CPSA) Qualification Requirements, Version 1.0, April 2019, page 10 PCI Card Production and Provisioning Template for Report on Compliance, Version 1.0, April 2019, page 3 PCI Card Production and Provisioning Attestation of Compliance, Version 1.0, April 2019, page 22

**NEW QUESTION 36**

If a vendor plans to terminate an employee, which of these must be done?

* The employee must be escorted from the premises immediately
* The employee’s locker and desk must be searched prior to termination
* The Human Resources department must be notified prior to termination
* The security manager must be notified in writing prior to termination

Explanation

According to the PCI Card Production Logical Security Requirements, the vendor must have a formal employee termination process that includes notifying the security manager in writing prior to the termination of any employee who has access to cardholder data or sensitive authentication data. This is to ensure that the security manager can take appropriate actions to revoke the employee’s access rights, credentials, and keys, and to prevent any unauthorized use or disclosure of cardholder data or sensitive authentication data by the terminated employee. The vendor must also have a documented policy and procedure for the employee termination process, and must maintain a log of all termination activities. References:

PCI Card Production Logical Security Requirements, v2.0, April 2019, page 19, requirement 6.1.2 PCI Card Production Logical Security Requirements, v2.0, April 2019, page 20, requirement 6.1.3

**NEW QUESTION 37**

Under which circumstances may boxes containing card stock remain unsealed within the vault?

* Where stock from those boxes will be pulled multiple times per day
* Where the stock from those boxes will be pulled once at the beginning of production
* Always, as long as an accurate inventory is being maintained
* This is never permitted

Explanation

According to the PCI Card Production and Provisioning Physical Security Requirements, the vendor must ensure that all boxes containing card stock are sealed with tamper-evident tape or labels when stored in the vault. The vendor must also maintain a log of all card stock movements in and out of the vault, and reconcile the card stock inventory at least daily. The vendor must not leave any boxes containing card stock unsealed within the vault, regardless of the frequency of stock pulling, as this may compromise the

security and integrity of the card stock and increase the risk of unauthorized access or theft. References: PCI Card Production and Provisioning Physical Security Requirements and Test Procedures v3.0, January 2022, pages

12-131

**Prepare With Top Rated High-quality CPSA_P_New Dumps For Success in Exam:**
https://www.actualtests4sure.com/CPSA_P_New-test-questions.html]