NMDPS NATIONAL CRIME INFORMATION CENTER (NCIC) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://nmpdsncic.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 16

SAMPLE

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

SAMPLE

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

SAMPLE

Questions

SAMPLE

1. **What should be done first when a security incident is detected?**
   - A. Notify the media
   - B. Leave the system alone
   - C. Report it to the appropriate authority
   - D. Attempt to resolve it independently

2. **Which of the following NCIC files is focused on firearm-related data?**
   - A. The Gun file
   - B. The Weapons file
   - C. The Firearms Registration file
   - D. The Ammunition file

3. **What are criminal justice agencies encouraged to implement concerning their internal security?**
   - A. Standardized national training
   - B. Policies tailored to local needs
   - C. General awareness programs
   - D. Annual audits of security

4. **What should happen to hard copies of FBI CJIS data/CHRI when retention is no longer necessary?**
   - A. File away for future reference
   - B. Physically destroyed
   - C. Shredded and sent to a warehouse
   - D. Distributed to staff for review

5. **What code is used in the Protection Order file to indicate "The protected person is granted exclusive possession of the residence or household"?**
   - A. 01
   - B. 03
   - C. 05
   - D. 04

SAMPLE

6. Can users disseminate FBI CJIS data for any governmental purposes?

A. Yes, they can

B. No, only specific purposes

C. Only for criminal investigations

D. Only at the request of supervisors

7. Can private citizens access the NCIC database directly?

A. Yes, with a valid reason

B. No, access is restricted to law enforcement agencies

C. Only through a legal representative

D. Yes, but only for criminal background checks

8. What is the minimum password length required for systems procured after September 30, 2005?

A. Ten characters

B. Fifteen characters

C. Twenty characters

D. Twenty-five characters

9. How many characters can certain fields in an NCIC record typically accommodate?

A. 100 characters

B. 80 characters

C. 50 characters

D. 120 characters

10. Which statement is true regarding Purpose Code I?

A. It can be used by any agency in the state

B. It may only be used by 1 authorized agency in each state

C. It can be used without restrictions by local agencies

D. It is open for public use for any purpose

SAMPLE

Answers

SAMPLE

1. C
2. A
3. B
4. B
5. B
6. B
7. B
8. C
9. B
10. B

SAMPLE

Explanations

SAMPLE

1. What should be done first when a security incident is detected?

A. Notify the media

B. Leave the system alone

C. Report it to the appropriate authority

D. Attempt to resolve it independently

When a security incident is detected, the first action should be to report it to the appropriate authority. This step is crucial for several reasons. First, notifying the right personnel allows for a coordinated response to the incident, ensuring that those who are trained and equipped to handle such situations can take immediate action. It helps in assessing the severity of the incident and determining the potential impact on the organization. Reporting the incident also facilitates proper documentation and investigation processes that may be necessary to understand the breach and prevent future occurrences. It allows for the engagement of cybersecurity professionals who can analyze the issue thoroughly and implement the necessary security measures. Leaving the system alone, notifying the media, or attempting to resolve the issue independently can lead to further complications, such as additional data loss, exposure of sensitive information, or legal ramifications if the incident is not handled appropriately. It's essential to alert the relevant authorities who have the expertise to deal with such situations effectively.

2. Which of the following NCIC files is focused on firearm-related data?

A. The Gun file

B. The Weapons file

C. The Firearms Registration file

D. The Ammunition file

The Gun file is specifically designed to contain firearm-related data, including information about stolen firearms, recovered firearms, and firearms suspected to be involved in criminal activity. This file is crucial for law enforcement, as it helps track and manage firearms in relation to criminal investigations. Understanding the role of the Gun file is vital for law enforcement officers and agencies, as it simplifies the process of retrieving important firearm-related information quickly and efficiently. Other options may reference firearms or ammunition, but they do not specifically denote a comprehensive database focused solely on firearms as the Gun file does. The Weapons file may be broader, potentially covering various types of weapons, while the Firearms Registration file would deal primarily with the registration status of firearms rather than the broader context of firearm-related crimes or incidents. The Ammunition file would specifically address data about ammunition rather than firearms themselves.

SAMPLE

3. What are criminal justice agencies encouraged to implement concerning their internal security?

A. Standardized national training

B. Policies tailored to local needs

C. General awareness programs

D. Annual audits of security

Criminal justice agencies are encouraged to implement policies tailored to local needs because each agency operates within a unique social, cultural, and legal context that influences how they manage internal security. Tailoring these policies ensures that the specific risks, challenges, and community concerns are adequately addressed, facilitating a more effective and responsive approach to security. By focusing on local needs, agencies can develop strategies and protocols that not only comply with overarching standards and regulations but also resonate with the day-to-day realities faced by law enforcement and justice professionals in their particular areas. This localized approach promotes higher efficiency, accountability, and trust within the community that the agency serves, ultimately contributing to better outcomes in crime prevention and response. In contrast, while standardized national training, general awareness programs, and annual audits of security are important components of overall security strategy, they do not offer the same level of customization and local relevance that policies tailored to specific needs provide.

4. What should happen to hard copies of FBI CJIS data/CHRI when retention is no longer necessary?

A. File away for future reference

B. Physically destroyed

C. Shredded and sent to a warehouse

D. Distributed to staff for review

When retention of hard copies of FBI Criminal Justice Information Services (CJIS) data or Criminal History Record Information (CHRI) is no longer necessary, the correct procedure is to ensure that these documents are physically destroyed. This step is crucial to maintain the integrity and confidentiality of sensitive information. Proper destruction mitigates the risk of unauthorized access to potentially harmful or private data that could be exploited if the documents were not disposed of securely. Physical destruction such as shredding ensures that the information cannot be reconstructed or retrieved, complying with stringent federal guidelines surrounding the handling of criminal justice information. This procedure not only protects individuals' privacy rights but also upholds the credibility of law enforcement agencies that handle such sensitive data. Other approaches, such as filing them away or distributing them to staff, do not provide the necessary security for confidential data and could lead to potential breaches of sensitive information. Similarly, shredding and sending to a warehouse introduces unnecessary risks, as the data could still be accessed if not completely destroyed. Thus, physical destruction is the only method that aligns with the protocols established by the FBI's CJIS Security Policy.

SAMPLE

5. What code is used in the Protection Order file to indicate "The protected person is granted exclusive possession of the residence or household"?

A. 01

B. 03

C. 05

D. 04

The correct code for indicating that "The protected person is granted exclusive possession of the residence or household" is indeed represented by the code associated with this specific legal protective measure. This code is part of the Protection Order file, which details the conditions and stipulations of enforced protection orders. In this context, the choice identified correctly corresponds to the legal terminology used within the National Crime Information Center (NCIC) framework. Each code is assigned a specific meaning to ensure clarity and consistency when reporting and accessing information regarding protection orders. By utilizing the designated code, law enforcement can swiftly understand the conditions attached to a protection order, facilitating more effective enforcement and adherence to the legal protections granted. The other options do not align with the definition of exclusive possession as defined by state or federal guidelines, making them unsuitable for representing this specific legal protection. Therefore, the chosen code effectively communicates the intent behind the protection order, recognizing the importance of exclusive possession for the safety of the protected individual.

6. Can users disseminate FBI CJIS data for any governmental purposes?

A. Yes, they can

B. No, only specific purposes

C. Only for criminal investigations

D. Only at the request of supervisors

The dissemination of FBI CJIS data is highly regulated to maintain the integrity and confidentiality of sensitive information. Users are only allowed to share this data for specific purposes that adhere to established guidelines. These guidelines are designed to ensure that the information is used responsibly and only in contexts where it is deemed necessary for maintaining public safety and law enforcement operations. This specificity in permissible use safeguards against potential misuse of the information, emphasizing that any sharing of CJIS data must serve a legitimate governmental function. By restricting dissemination to specific purposes, the policies help protect the privacy of individuals and uphold the proper use of law enforcement resources.

7. Can private citizens access the NCIC database directly?

A. Yes, with a valid reason

B. No, access is restricted to law enforcement agencies

C. Only through a legal representative

D. Yes, but only for criminal background checks

Access to the NCIC database is strictly limited to law enforcement agencies and certain authorized personnel within those agencies. This restriction is in place to ensure the security and integrity of sensitive information, which is primarily used to assist law enforcement in the performance of their duties, such as locating missing persons, identifying stolen property, or investigating criminal activity. The nature of the information housed within the NCIC is such that it involves ongoing investigations and sensitive law enforcement matters that should not be available to the general public. Allowing private citizens direct access to such information could lead to misuse, unethical behavior, or compromise ongoing investigations. The other options imply varying degrees of access that do not align with the established protocols and regulations surrounding the NCIC database. Therefore, the correct understanding is that access is indeed restricted to authorized law enforcement personnel only.

EXAMPLE

8. What is the minimum password length required for systems procured after September 30, 2005?

A. Ten characters

B. Fifteen characters

C. Twenty characters

D. Twenty-five characters

The minimum password length required for systems procured after September 30, 2005, is twenty characters. This requirement is in place to enhance the security of systems against unauthorized access. Longer passwords are generally more difficult to guess or crack through brute force methods. Establishing a minimum password length of twenty characters significantly increases the strength of user authentication. Many security protocols recommend this standard to protect sensitive information, making it imperative for organizations to implement and adhere to these guidelines when procuring new systems. By enforcing a higher character count, organizations can ensure that employee and system passwords are more resilient against both dictionary attacks and various forms of cyber threats, ultimately leading to a safer cybersecurity posture.

9. How many characters can certain fields in an NCIC record typically accommodate?

A. 100 characters

B. 80 characters

C. 50 characters

D. 120 characters

The correct answer indicates that certain fields in an NCIC record can typically accommodate 80 characters. This standard is established to ensure that the necessary data can be recorded without overwhelming the system and maintaining clarity. The 80-character limit allows for concise entries while still providing adequate space for essential information. In many systems, including NCIC, the design of data fields is crucial for effective communication and data retrieval. The decision to set limits on character counts is often influenced by the need for efficiency and consistency across records. This 80-character limit helps in maintaining uniformity and ensures that all data can be processed systematically within the database constraints and interfacing systems. Understanding this character limit is essential, as it ensures that personnel inputting data do so thoughtfully, adhering to formatting requirements, which ultimately leads to better data management and retrieval for law enforcement and other agencies relying on NCIC records.

SAMPLE

10. Which statement is true regarding Purpose Code I?

A. It can be used by any agency in the state

B. It may only be used by 1 authorized agency in each state

C. It can be used without restrictions by local agencies

D. It is open for public use for any purpose

Purpose Code I is specifically designed for use by authorized agencies to facilitate inquiries regarding criminal justice. The correct answer reflects that it may only be utilized by one authorized agency in each state, underscoring the exclusivity and limitations placed on its access. This code was instituted to ensure that sensitive information and records related to criminal justice are accessed and utilized by designated bodies, thereby maintaining data integrity and protecting the privacy of individuals involved. The restriction to one authorized agency per state helps to streamline a controlled and accountable use of the system, preventing misuse or overexposure of critical data. The other options suggest broader accessibility than is allowed under Purpose Code I. The idea that it could be used by any agency or without restrictions by local agencies indicates a misunderstanding of these designed limitations, which are crucial for maintaining proper oversight in the handling of criminal justice information. Additionally, public use of this purpose code is not endorsed, as such information is intended for use only within the confines of those authorized to do so under specific legal frameworks.

SAMPLE

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://nmpdsncic.examzify.com

We wish you the very best on your exam journey. You've got this!

SAMPLE