I'll create 36 exam questions based on the content provided from Chapter 5, following your requirements.

**Chapter 5 Exam Questions**

**Questions**

1. What is the first step in any asset management process?   
   A) Setting up baselines B) Making an inventory of all assets C) Implementing security controls D) Conducting risk assessment
2. Which data classification level would be appropriate for information that is already public or intended for public release?   
   A) Highly restricted B) Moderately restricted C) Low sensitivity D) Unrestricted/Public data
3. What is data remanence?   
   A) The process of data encryption B) The residual data that might remain on a device after deletion C) A method of data classification D) The process of backing up data
4. In the context of symmetric encryption, what is a key challenge?   
   A) It's too slow for everyday use B) It requires a large number of keys as users increase C) It's not suitable for securing sensitive data D) It cannot be used for bulk data encryption
5. Which encryption method uses different keys for encryption and decryption?   
   A) Symmetric encryption B) Asymmetric encryption C) Hash encryption D) Substitution cipher
6. What is the main purpose of "salting" in the context of password hashing?   
   A) To make passwords easier to remember B) To prevent attacks using precomputed hash tables C) To encrypt the original password D) To comply with regulatory requirements
7. What does the "purging" method aim to accomplish in data destruction?   
   A) Reclassify data sensitivity levels B) Back up data before deletion C) Eliminate or greatly reduce the chance of recovering residual data D) Transfer data to a secondary storage location
8. Which of the following is NOT typically included in a password policy?   
   A) Password complexity requirements B) Password expiration timeframes C) Employee salary information D) Responsibility for policy enforcement
9. What is a primary benefit of data classification?   
   A) It makes data processing faster B) It leads to more efficient design and implementation of security processes C) It reduces the amount of data stored D) It eliminates the need for encryption
10. Which type of social engineering attack specifically targets high-profile employees like CEOs or CFOs?   
    A) Vishing B) Pretexting C) Whaling D) Quid pro quo
11. What is "egress monitoring" used for?   
    A) Monitoring all inbound communications traffic B) Regulating data leaving the organization's IT environment C) Tracking employee work hours D) Securing the physical perimeter of the organization
12. In change management, what does RFC stand for?   
    A) Ready For Change B) Request For Change C) Reason For Change D) Response From Client
13. What is the process of applying the hash function multiple times called?   
    A) Multi-hashing B) Recursive hashing C) Key stretching D) Hash pipelining
14. What is the primary disadvantage of asymmetric encryption compared to symmetric encryption?   
    A) It requires more storage space B) It is slower due to larger keys and more intensive mathematical operations C) It requires more frequent key changes D) It is more vulnerable to brute force attacks
15. Which of the following is NOT a typical component of security awareness training?   
    A) Education B) Training C) Awareness D) Certification
16. What is "tailgating" in the context of social engineering?   
    A) Following an authorized user into a restricted area B) Sending multiple phishing emails to the same target C) Monitoring a user's internet activity D) Installing unauthorized software on a system
17. Which data handling process identifies potential organizational impacts if data suffers security compromises?   
    A) Labeling B) Retention C) Classification D) Destruction
18. What is a baseline in configuration management?   
    A) The minimum security requirements for a system B) A comprehensive inventory of all a system's components C) The regular update schedule for patches D) The process of testing system modifications
19. What should be done before implementing a patch across an organization?   
    A) Notify all employees via email B) Update the organization's security policy C) Test the patch to ensure it doesn't negatively affect system functionality D) Get approval from every department head
20. What is the purpose of regression testing in update management?   
    A) To verify that newly installed functionality works as intended B) To ensure modifications did not introduce unexpected behaviors C) To determine if users can adapt to the changes D) To measure the performance impact of updates
21. Which policy allows employees to use their personal devices for work purposes?   
    A) Acceptable Use Policy (AUP) B) Bring Your Own Device (BYOD) Policy C) Data Classification Policy D) Password Policy
22. What is the purpose of having a rollback plan in patch management?   
    A) To reverse changes if a patch causes problems B) To schedule regular system backups C) To document who approved the patch D) To inform users of upcoming changes
23. Which encryption method is most suitable for encrypting large amounts of data like backups or hard drives?   
    A) Asymmetric encryption B) Hashing C) Symmetric encryption D) Digital signatures
24. What is "vishing" in the context of social engineering?   
    A) Using video calls to trick users B) Phone phishing using fraudulent interactive voice response systems C) Sending malicious links through text messages D) Creating fake websites to collect login credentials
25. In the data handling lifecycle, what follows "Processing"?   
    A) Creation B) Storage C) Transmission D) Destruction
26. What is a common mistake in records retention policies?   
    A) Not keeping any records B) Applying the longest retention period to all types of information C) Storing all records in a single location D) Allowing all employees access to all records
27. Which of the following is NOT typically covered in an Acceptable Use Policy (AUP)?   
    A) Data access B) Password management C) Employee compensation D) Internet usage rules
28. What should an organization do with records and information that are no longer required?   
    A) Archive them indefinitely B) Transfer them to cloud storage C) Destroy them in accordance with policies and legal requirements D) Convert them to a different format
29. What does a change management policy primarily focus on?   
    A) Hiring new employees B) The decision-making process for implementing changes C) Upgrading hardware components D) User training programs
30. Which component of security awareness addresses how employees' actions align with information security goals?   
    A) Risk assessment B) Compliance training C) Understanding expectations D) Technical skills development
31. What problem does asymmetric encryption solve compared to symmetric encryption?   
    A) Speed of encryption B) Complexity of algorithms C) Key distribution D) Storage requirements
32. Which data classification level is applied to data whose compromise could lead to temporary loss of competitive advantage?   
    A) Highly Restricted B) Moderately Restricted C) Low Sensitivity D) Unrestricted
33. What is the recommended practice for protecting passwords?   
    A) Writing them down and storing them in a desk drawer B) Using the same password for multiple systems C) Using a secure password manager D) Sharing them with technical support when needed
34. What is a "pepper" in the context of password security?   
    A) A random value added to the password before hashing and not stored in the database B) A type of multi-factor authentication C) A method to recover forgotten passwords D) A technique to encrypt database connections
35. What is the main purpose of a privacy policy in an organization?   
    A) To enforce password complexity requirements B) To define what is considered PII/ePHI and detail appropriate handling procedures C) To establish procedures for system updates D) To outline approved usage of IT infrastructure
36. In configuration management, what is the purpose of acceptance testing?   
    A) To verify that newly installed functionality works as intended B) To ensure that all users accept the changes C) To determine if changes are necessary D) To classify the severity of security vulnerabilities

**Answers**

1. B) Making an inventory of all assets
   * Explanation: As stated in the content, "Making an inventory, catalog, or registry of all the organization's information assets is the first step in any asset management process." This aligns with the principle "You can't protect what you don't know you have."
2. D) Unrestricted/Public data
   * Explanation: The document defines "Unrestricted/Public Data" as data that "is already publicly available or intended for public release. No harm can come from further dissemination or disclosure of this data, as it's intended for public consumption."
3. B) The residual data that might remain on a device after deletion
   * Explanation: As defined in the document, "Data remanence refers to the residual data that might remain on a device even after data deletion. This residual data could pose significant security threats if not addressed properly."
4. B) It requires a large number of keys as users increase
   * Explanation: The document states that "the scalability of symmetric encryption is challenging because the number of keys grows rapidly as the number of different users or groups increases," giving the example that an organization of 1,000 employees would need 499,500 keys.
5. B) Asymmetric encryption
   * Explanation: The document defines asymmetric encryption as using "one key to encrypt and a different key to decrypt the input plaintext, as opposed to symmetric encryption that uses the same key for both encryption and decryption."
6. B) To prevent attacks using precomputed hash tables
   * Explanation: The document explains that "to prevent attacks using precomputed tables of hashes (rainbow tables), a random value called a 'salt' is often added to the password before hashing."
7. C) Eliminate or greatly reduce the chance of recovering residual data
   * Explanation: According to the document, purging "eliminates or greatly reduces the chance of recovering residual data from the original values, even after the system has been cleared."
8. C) Employee salary information
   * Explanation: The document states that a password policy should include expectations for systems and users, leadership commitment, standards for creating passwords, and who is responsible for enforcement. Employee salary information is not related to password policies.
9. B) It leads to more efficient design and implementation of security processes
   * Explanation: The document states that "Classification can lead to a more efficient design and implementation of security processes. If data with similar classifications can be protected using the same controls strategy, this can streamline security processes and make them more effective."
10. C) Whaling
    * Explanation: The document defines whaling attacks as "a type of phishing attack that specifically targets high-profile employees, such as the CEO or CFO, in order to steal sensitive information from a company."
11. B) Regulating data leaving the organization's IT environment
    * Explanation: According to the document, "Egress monitoring is used to regulate data leaving the organization's IT environment, often through Data Loss Prevention (DLP) or Data Leak Protection solutions."
12. B) Request For Change
    * Explanation: The document states that "Change management starts with a Request for Change (RFC). This could be due to an identified need for system enhancement, to rectify a detected problem, or to introduce new functionality."
13. C) Key stretching
    * Explanation: The document explains that "to increase the computational cost of generating hashes (and thus slow down attackers), many systems apply the hash function multiple times in what's known as key stretching."
14. B) It is slower due to larger keys and more intensive mathematical operations
    * Explanation: The document states that "The main disadvantage of asymmetric encryption is its slowness compared to symmetric encryption due to its handling of much larger keys and more intensive mathematical operations."
15. D) Certification
    * Explanation: According to the document, security awareness training includes three components: Education, Training, and Awareness. Certification is not mentioned as a component.
16. A) Following an authorized user into a restricted area
    * Explanation: The document defines tailgating as a tactic that "involves following an authorized user into a restricted area or system," giving the example of someone asking you to hold the door open because they forgot their company RFID card.
17. C) Classification
    * Explanation: The document defines classification as "a process that identifies the potential organizational impacts if data suffers any security compromises, particularly relating to its confidentiality, integrity, and availability."
18. B) A comprehensive inventory of all a system's components
    * Explanation: The document defines a baseline as "a comprehensive inventory of all a system's components including hardware, software, data, administrative controls, documentation, and user instructions."
19. C) Test the patch to ensure it doesn't negatively affect system functionality
    * Explanation: The document states that "Before implementing a patch across an organization, it should be tested to ensure it doesn't negatively affect system functionality."
20. B) To ensure modifications did not introduce unexpected behaviors
    * Explanation: According to the document, regression testing "ensures that the modifications did not introduce any unexpected or erroneous behaviors into the system."
21. B) Bring Your Own Device (BYOD) Policy
    * Explanation: The document states that a "Bring Your Own Device (BYOD) policy allows employees to use their personal devices for work purposes."
22. A) To reverse changes if a patch causes problems
    * Explanation: The document explains that "If a patch causes problems, it may be necessary to rollback the system to a previous state before the patch was applied. It's important to have a documented rollback plan ready in case it's needed."
23. C) Symmetric encryption
    * Explanation: The document states that symmetric encryption is used for "Encrypting bulk data, such as backups, hard drives, and portable media."
24. B) Phone phishing using fraudulent interactive voice response systems
    * Explanation: The document defines vishing (phone phishing) as involving "the use of a fraudulent interactive voice response (IVR) system that mimics the IVR system of a legitimate institution."
25. B) Storage
    * Explanation: According to the lifecycle of data provided in the document, the order is: Creation, Processing, Storage, Transmission, Access, Archiving, Destruction/Disposal.
26. B) Applying the longest retention period to all types of information
    * Explanation: The document identifies a common mistake as "applying the longest retention period to all types of information in an organization," which "increases storage costs and risks of data exposure, adds noise when searching for relevant records, and may violate externally mandated requirements."
27. C) Employee compensation
    * Explanation: The document lists common aspects covered in AUPs including data access, system access, data disclosure, password management, data retention policies, Internet usage rules, and guidelines for company device usage. Employee compensation is not mentioned.
28. C) Destroy them in accordance with policies and legal requirements
    * Explanation: The document states that "Records and information no longer required should be destroyed in accordance with the enterprise's policies and any applicable legal requirements."
29. B) The decision-making process for implementing changes
    * Explanation: The document states that "Change management focuses on the decision-making process, which results in giving approvals to system support teams, developers, and end users to implement the proposed changes."
30. C) Understanding expectations
    * Explanation: The document states that "Awareness training educates employees about the expectations the organization has for them regarding their responsibilities and accountabilities."
31. C) Key distribution
    * Explanation: The document explains that "Asymmetric encryption solves the problem of key distribution by allowing secure message transfer across an untrusted medium without needing prior key exchange or key material distribution."
32. B) Moderately Restricted
    * Explanation: The document defines "Moderately Restricted" as being "applied to data whose compromise could lead to temporary loss of competitive advantage, financial loss, or disruption of planned investments or activities."
33. C) Using a secure password manager
    * Explanation: The document states that "Password managers are tools that can store multiple passwords securely" and that "Organizations should encourage unique passwords for each system and recommend a reliable password management solution."
34. A) A random value added to the password before hashing and not stored in the database
    * Explanation: The document explains that "peppering involves adding a secret value before hashing. The 'pepper' is not stored in the database, adding another layer of security if the database is compromised."
35. B) To define what is considered PII/ePHI and detail appropriate handling procedures
    * Explanation: The document states that "The organization's privacy policy should define what is considered PII/ePHI. It should also detail appropriate handling procedures and mechanisms, user expectations, enforcement mechanisms, and punitive measures for non-compliance."
36. A) To verify that newly installed functionality works as intended
    * Explanation: The document states that "Any modifications, updates, or repairs must be acceptance tested. This testing verifies that newly installed functionality works as intended."