Here’s your **comprehensive sentence-by-sentence breakdown** of the Encryption Best Practices document, formatted for professional Word use with numbering, minimal spacing, and all essential details preserved and explained.

**Encryption Best Practices – Detailed Study Notes**

1. **Role of Encryption in Data Security**
   * Encryption is a proven method for securing data.
   * Focus in this lesson: encryption concepts, not specific algorithms (e.g., DES, IDEA, AES).
   * Two main categories of data: **unencrypted** and **encrypted**.
2. **Unencrypted Data (Cleartext / Plaintext)**
   * Data stored, transmitted, or processed in an unprotected, readable format.
   * Example: Transmitting a username and password in plain text (e.g., logging into a Telnet server) exposes it to interception via packet capture.
3. **Encrypted Data (Ciphertext)**
   * Data encoded so it can only be read with the correct decryption key.
   * Without the key, encrypted data remains unreadable.
   * Encryption mitigates risk by protecting confidentiality even if access controls are bypassed.
4. **Three Data States**
   * **Data at Rest**: Stored on memory, hard drives, or other storage devices.
   * **Data in Transit (Data in Motion)**: Moving between systems or within system components.
   * **Data in Use (Data in Processing)**: Actively processed in memory or CPU.
5. **Data at Rest**
   * Examples: Files stored on an external hard drive.
   * Protection:
     + Full disk encryption (e.g., BitLocker).
     + Folder- or file-level encryption.
     + Database encryption.
   * Goal: Prevent unauthorized reading of stored data without the decryption key.
6. **Data in Transit / Data in Motion**
   * Includes data sent across networks or between system components (e.g., hard disk → memory → CPU).
   * Examples of protection methods:
     + TLS/SSL for secure web applications.
     + IPsec or L2TP for VPN connections.
     + WPA2 with AES for wireless encryption.
   * Objective: Maintain confidentiality during transfer between endpoints.
7. **Data in Use / Data in Processing**
   * Active, non-persistent data in RAM, CPU cache, or CPU registers.
   * Example: Decrypted files temporarily stored in memory while being worked on.
   * Protection: Some CPUs (e.g., AMD, Intel) implement secure processing with encryption and integrity checks.
8. **Example Scenario – Data State Transitions**
   * File with exam results stored encrypted on a hard drive → **Data at Rest**.
   * Decryption to plaintext for reading → temporarily **Data in Use**.
   * Sending result to a team member over Slack with HTTPS → **Data in Transit**.
   * Receiving user stores file again encrypted → returns to **Data at Rest**.
   * Demonstrates constant movement between data states and the need for protection in each.
9. **Key Security Principle**
   * Data moves continuously between at rest, in transit, and in use.
   * Must ensure encryption methods are applied appropriately for each state to maintain confidentiality.