Here’s your **comprehensive sentence-by-sentence breakdown** of the End-User Best Practices document, formatted for professional Word use with numbering, minimal spacing, and full retention of key details.

**End-User Best Practices – Detailed Study Notes**

1. **Purpose of End-User Best Practices**
   * Goal: Reduce security risks by implementing safe behavior when handling systems, hardware, and sensitive information.
   * Areas covered:
     + Logging off and locking systems.
     + Using screensaver locks.
     + Securing critical hardware (laptops, portable devices).
     + Protecting personally identifiable information (PII) and sensitive data (e.g., passwords).
2. **Logging Off vs. Locking the Computer**
   * Always log off or lock the computer when leaving it unattended.
   * **Log off**: If away for a long duration (e.g., lunch, end of day).
   * **Lock**: If away briefly (e.g., restroom break).
   * Both methods require re-entry of username and password before access is restored.
3. **Manual and Automatic Locking**
   * Automatic locking: Configurable via screensaver timeout (1–5 minutes typical).
   * Manual lock in Windows: Press Start + L.
   * MacOS: Use **Hot Corners** to quickly lock or log out by moving the cursor to a designated corner.
   * Training users to lock systems when leaving their desks is essential.
4. **Logging Out for Extended Absences**
   * Windows log out: Start button → Profile icon → Sign out.
   * Purpose: Allows the next authorized user to log in (important in shared or domain-based environments).
5. **Screensaver Lock Configuration**
   * Purpose: Automatically lock system after inactivity, requiring password to resume.
   * Setup: Start menu → Settings → Personalization → Lock screen → Screensaver settings.
   * Choose idle time (1–5 minutes) and check “On resume, display logon screen.”
6. **Securing Critical Hardware**
   * Laptops and mobile devices are prone to theft due to portability.
   * In-office: Use cable or laptop locks to secure to desks.
   * In public: Always keep devices in sight; take them with you if leaving your spot (e.g., in a café).
   * Avoid leaving devices unattended even briefly, as theft or tampering can occur within minutes.
7. **Securing PII(Personally Identifiable Information) and Sensitive Data**
   * PII examples: employee salary details, home addresses, family information.
   * Risks: Theft, unauthorized viewing, or copying.
   * Physical protection: Implement a **Clean Desk Policy**—store files in locked drawers or cabinets when not in use.
   * Digital protection: Encrypt sensitive files to restrict access to authorized users only.
8. **Importance of Dual Protection (Physical and Digital)**
   * Physical security prevents unauthorized access to tangible documents.
   * Encryption and access controls safeguard digital data against breaches.
9. **Summary of End-User Best Practices**
   * Lock or log off systems when unattended (duration-based decision).
   * Use screensaver locks with passwords.
   * Keep portable devices secured physically or in your possession at all times.
   * Protect PII and sensitive data both physically (locked storage) and digitally (encryption and access control).