Here is the **comprehensive sentence-by-sentence study note breakdown** of your document, formatted for professional Word use without unnecessary spacing. All key details are preserved and explained for maximum clarity.

**Account Management – Detailed Study Notes**

1. **Definition and Purpose of Account Management**
   * Account management is a set of policies used to determine the rights and privileges each user or employee has on a computer or network.
   * These policies are created by the organization and enforced by technicians through system configuration.
   * The goal is to allow legitimate actions while preventing unauthorized ones.
2. **Core Account Management Functions**
   * Restricting user permissions.
   * Changing the default administrator account and password.
   * Disabling guest accounts.
   * Restricting login times.
   * Configuring failed login attempt limits.
   * Limiting concurrent logins.
   * Using timeouts and screen locks.
3. **Restricting User Permissions (Least Privilege Principle)**
   * Assign only the minimum access rights required for a job.
   * Supports the “least privilege” security best practice, reducing attack surface.
   * Example: Students can access the internet but cannot open instructor-grade books.
   * Achieved through access control lists (ACLs) and permissions for files, folders, and devices.
   * File permissions control read, modify, or delete actions locally or over a network.
   * NTFS permissions handle local system control; shared permissions apply to network resources.
   * Hardware/software restrictions also apply (e.g., installing printers requires administrative rights).
4. **Changing the Default Administrator Account and Password**
   * New systems come with a **default** high-privilege account or super user:
     + Linux/Unix/MacOS: root user.
     + Windows: Administrator account.
   * These accounts have full control; attackers target them.
   * **Best practices for default administrative account**:
     + Set a long, strong password.
     + Disable the default account.
     + Create a named administrative account instead (e.g., “JohnAdmin”).
   * Prevents brute force, hybrid, or dictionary attacks on well-known default account names.
5. **Disabling Guest Accounts**
   * Guest accounts allow unauthenticated access, intended for temporary/basic use.
   * In older Windows versions (7, 8, 8.1), guest accounts were enabled by default – disable them for security.
   * In modern Windows, guest accounts are disabled by default due to vulnerabilities.
   * Create standard user accounts for tracking and accountability instead of using guest accounts.
6. **Restricting Login Times**
   * Default: users can log in at any time.
   * Security enhancement: limit logins to specific days/times (e.g., work hours).
   * Prevents unauthorized access during off-hours when security staff may be unavailable.
   * Can be set organization-wide or per user based on time zones.
   * Particularly effective in preventing foreign attackers from logging in at night when staff aren’t monitoring.
7. **Failed Login Attempt Lockouts**
   * Set a maximum number of incorrect password attempts before action is taken.
   * Common example: lockout after 3 failed attempts for 15 minutes.
   * Options:
     + **Disable account** – requires help desk intervention to unlock (most secure, but resource-heavy).
     + **Time-based lockout** – temporary block to slow down brute force attacks.
   * Timeouts greatly extend the time required for brute force attempts, discouraging attackers.
8. **Limiting Concurrent Logins**
   * In domain environments, a single account can log in to multiple machines simultaneously.
   * Risk: allows password sharing or unauthorized simultaneous access from multiple locations.
   * Security best practice: limit to one concurrent login per account.
   * Forces the user to log out before logging into another machine.
9. **Timeouts and Screen Locks**
   * Automatically lock a computer after inactivity, requiring reauthentication.
   * Short timers (e.g., 1 minute) are secure but can disrupt work; longer timers balance security and convenience.
   * Example: 5-minute timer allows short interruptions without constant re-logins.
   * Manual locking is ideal when stepping away, but timeouts serve as a safeguard if the user forgets.
10. **Summary – Seven Key Account Management Controls**
    * Restrict user permissions.
    * Change default administrator account and password.
    * Disable guest account.
    * Restrict login times.
    * Limit failed login attempts.
    * Restrict concurrent logins.
    * Use timeouts and screen locks.