Below is a **sentence-by-sentence analysis** of your *Security Principles Notes* document, rewritten into **professional study notes** with all critical information preserved. The format is designed for **clean pasting into Microsoft Word**, using minimal spacing, bullet points, and numbered topic headers.

**Security Principles – Study Notes - CompTIA A+ 220-1102 | Objective 2.1: Security Concepts**

**1. Principle of Least Privilege**

* **Definition:** Users and systems should be granted the minimum level of access necessary to perform their tasks.
* **User Example:**
  + A regular user should check emails with a standard user account, not an administrative one.
  + Administrative rights should only be used when performing tasks that require elevated privileges (e.g., installing software or changing configurations).
* **Applies to Systems/Networks:**
  + Least privilege is not limited to user accounts—it should be applied during system and network design.
* **IoT Device Example:**
  + Devices like smart LED lights should be isolated in a separate **subnet or VLAN**.
  + These devices should only have limited access (e.g., open a couple of ports or reach the internet for updates), not access to file servers, printers, etc.
  + Access should be **strictly controlled** in and out of the IoT VLAN.

**2. Access Control Models / Role Base Access**

**2.1 Discretionary Access Control (DAC)**

* **Definition:** Access is determined by the **owner** of the object (file/folder).
* **Use Case:** Common in shared environments like corporate file servers.
* **Advantages:**
  + Allows **granular control** by the object owner.
  + Owners are often most knowledgeable about access needs.
* **Challenges:**
  + Every object must have an **assigned owner**.
  + Permissions are only as good as the owner’s judgment.
  + If permissions are too tight: Users who need access may be denied.
  + If permissions are too loose: Sensitive data may be exposed.
* **Enterprise Caution:** In large organizations, DAC can be risky due to its user-dependent structure.

**2.2 Mandatory Access Control (MAC)**

* **Definition:** Access is determined by **the system**, not the object owner.
* **Mechanism:**
  + Assigns **security labels** (trust levels) to both **subjects (users)** and **objects (resources)**.
  + Access is granted when the user's label meets or exceeds the object's classification.
* **Military Use Case:**
  + Document levels: **Unclassified**, **Confidential**, **Secret**, **Top Secret**.
  + Personnel clearance determines access (e.g., a colonel may access top secret, secret, confidential, and unclassified documents).
* **Need to Know Principle:**
  + Even with proper clearance, a user must demonstrate a **"need to know"** to access a specific resource.
* **Complexity:**
  + Labeling system can be deeply nested and complex.
  + Not typically used in enterprises, mainly in **military and intelligence agencies**.

**2.3 Role-Based Access Control (RBAC)**

* **Definition:** Access is based on **roles** assigned to users and resources.
* **Mechanism:**
  + Instead of setting permissions per individual, permissions are set by **job roles** (e.g., Sales, HR, IT).
  + Files/folders are tied to role permissions, and users are added/removed from roles as needed.
* **Best Practice in Cybersecurity:**
  + Avoids manually assigning permissions per user.
  + Supports **least privilege** by granting access based only on job necessity.
* **Example:**
  + IT team may need access to all departments’ data for backups.
  + Sales team only accesses sales files, not HR or IT files.
* **Windows Power Users Example:**
  + Power Users can perform tasks like changing the time or adding a printer but do not have full admin rights.
  + Useful middle ground between **user** and **administrator** **roles**.

**3. Zero Trust Security Model**

* **Definition:** A framework that assumes **no inherent trust**—all users, devices, and access requests must be **authenticated**, **authorized**, and **continuously validated**.
* **Reason for Adoption:**
  + Traditional network perimeters are dissolving due to:
    - Cloud services
    - Bring Your Own Device (BYOD)
    - Remote work
  + Trust boundaries are now **blurry**, not well-defined like with legacy firewalls or border routers.
* **Assumption:** Every user or device—**inside or outside** the organization—could be a potential threat.

**4. Zero Trust Implementation – Four Key Principles**

**4.1 Reexamine Default Access Controls:**

* No device or user is automatically trusted.
* All traffic must be authenticated and validated—even internal traffic.

**4.2 Use Layered Defense Mechanisms:**

* Employ multiple security methods such as:
  + Multi-Factor Authentication (MFA)
  + Data Loss Prevention (DLP)
  + Microsegmentation
  + Least privilege enforcement

**4.3 Enable Real-Time Monitoring:**

* Use tools like SIEMs (Security Information and Event Management) and EDR (Endpoint Detection & Response) to:
  + Detect malicious activity
  + Stop threats as they occur

**4.4 Align Architecture to Security Strategy:**

* Replace outdated systems.
* Build reliance on **modern endpoint monitoring and response** technologies.
* Enhance network resilience for future security incidents.

**5. Summary of Key Security Principles**

| **Principle** | **Description** |
| --- | --- |
| Least Privilege | Limit user/system access to what is strictly necessary |
| DAC | Owner-controlled access, common but riskier in large organizations |
| MAC | System-controlled access using classification labels (e.g., military use) |
| RBAC | Access determined by user roles/job functions (cybersecurity best practice) |
| Zero Trust | No implicit trust; every user/device must prove identity and need-to-know |