Below is a **comprehensive sentence-by-sentence breakdown** of your uploaded document *“Physical Access Controls Notes.docx”*, formatted as **professionally structured study notes** for **Microsoft Word**. This breakdown includes all critical details and aligns with **CompTIA A+ 220-1102 Objective 2.1**.

**Physical Access Controls – Study Notes (CompTIA A+ 220-1102, Objective 2.1)**

**1. Door Locks**

* **1.1 Five Types of Door Locks:**
  + Key-operated
  + Mechanically operated
  + Electronically operated
  + Badge readers
  + Biometric door locks

**1.2 Key-Operated Locks:**

* Traditional door lock using a **physical key**.
* Common in **residential and basic office use**.
* Requires turning the key and then using the **handle** to open the door.

**1.3 Mechanically Operated Locks (Cipher Locks):**

* Use **PIN numbers** instead of physical keys.
* Operate via **mechanical tumblers**, not electronic.
* Do **not require electricity or batteries meaning power**.

**1.4 Electronically Operated Locks:**

* Use **PINs or passwords** entered on an **electronic keypad**.
* Require **power**, usually via **rechargeable or replaceable batteries**.
* Key difference from mechanical: **power dependency**.

**1.5 Badge Reader Locks:**

* Use **smart cards** or **RFID fobs** to authenticate.
* May combine **Identification** **badge with an embedded RFID chip + PIN Number** for **two-factor authentication**.
  + Use some sort of token like a smart card or an RFID-Based Key fob to be able to unlock that door.
  + Accessing office building by swiping badge and then enter the pin number.
* Common in **military, government, and large enterprises**.

**1.6 Biometric Door Locks:**

* Use unique **biometric identifiers** like:
  + **Fingerprint**
  + **Palm print**
  + **Retina**
  + **Facial recognition**

**2. Biometric Methods**

**2.1 Fingerprint Scanners:**

* Use a **capacitive cell** to detect ridge patterns.
  + If your finger print matches the one that’s stored inside of its memory it will then unlock the device.
* **Quick and non-intrusive**, but:
  + Raise **hygiene concerns** (dirt, bacteria).
  + Require **frequent cleaning**, especially on shared devices.

**2.2 Palm Print Scanners:**

* Larger than fingerprint readers.
* Use **infrared or visible light** to read **vein and blood vessel patterns**.
* Devices are **bulkier**, requiring external connection to door lock.
* Also raise hygiene issues.

**2.3 Retina Scanners:**

* Use **infrared light** to scan **blood vessel patterns** in the eye.
* Require **close contact** — considered **highly intrusive**.
* Used in **high-security (top-secret) environments**.
* Rare in standard offices.

**2.4 Facial Recognition:**

* Uses cameras to scan **facial structure**.
* Least intrusive biometric method.
* Compares facial images to stored authorized data.
* Ideal for quick identification with **no physical contact**.

**2.5 Biometric Intrusiveness Ranking (Least to Most):**

1. Facial recognition
2. Fingerprint
3. Palm print
4. Retina scan

**3. Equipment Locks**

**3.1 Purpose:**

* Prevent **unauthorized physical access** to:
  + Servers
  + Network appliances
  + Critical devices

**3.2 Lockable Rack Cabinets (Networking / Servers):**

* Most common equipment lock.
* Enclose multiple devices (e.g., 4–20 units per rack).
* May use:
  + **Key lock**
  + **PIN pad**
  + **Biometric (fingerprint/facial ID)**

**3.3 Chassis Locks & Faceplates:**

* Also used in server racks or networking racks for layering protection.
* Provide **secondary protection** by securing each individual server inside the cabinet.
* Prevent removal or tampering if someone gains access to the rack.

**3.4 Kensington Locks:**

* Function like **bike locks** for IT equipment.
* Secure **portable devices** (e.g., laptops) to immovable objects.
* Attach to:
  + **Desks**
  + **Pillars**
  + **Bookshelves**

**4. Access Control Vestibules (Formerly “Mantraps”)**

**4.1 Purpose:**

* Control the **flow of personnel** in/out of secure areas.
* Act as a **choke point** between public and private space.

**4.2 Real-World Analogy:**

* Similar to **subway turnstiles** requiring a **token or card** to pass through.

**4.3 Types of Vestibules:**

* **Turnstiles**
* **Full-cage systems** with:
  + Authentication step (PIN, badge, etc.)
  + Two-door sequence (enter, authenticate, exit)

**4.4 Use Cases:**

* Common in **corporate, government, and military facilities**.
* Prevent **piggybacking** and **tailgating**.
* Enforce **one-person-at-a-time access**.

**5. Badge Readers**

**5.1 Use Cases:**

* Employed at:
  + Building entrances
  + Parking garages
  + Access control vestibules
  + Computer login terminals

**5.2 Badge Technologies:**

* **Magnetic Stripe:**
  + Swipe-style badge (like older credit cards).
* **Smart Cards:**
  + Contain embedded **microchips**.
  + Often require **PIN for two-factor authentication**.
* **RFID Badges:**
  + Use **radio frequencies** for contact/contactless access.
  + Can be read:
    - **By touch**
    - **Within a few inches to 1 foot**, depending on system.

**5.3 RFID Badge Reader Types:**

* **Contact-based:** Touch to reader.
* **Contactless:** Near-field communication.

**6. Summary – Physical Access Controls Overview**

* **Door Locks:** Secure rooms via key, PIN, badge, or biometrics.
* **Biometrics:** Provide unique ID via physical traits.
* **Equipment Locks:** Secure IT devices at rack and chassis level.
* **Access Control Vestibules:** Control traffic and prevent unauthorized entry.
* **Badge Readers:** Authenticate identity using magnetic, smart card, or RFID methods.