Below is a **sentence-by-sentence, fully detailed breakdown** of the document *“Security Controls Notes.docx”*, formatted as **structured study notes** for pasting directly into **Microsoft Word**. It maintains professional formatting, minimal spacing, and clear bullet structure aligned with **CompTIA A+ 220-1102 Objective 2.1**.

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

**1. Overview of Security Control Types**

* Security controls are essential tools used by system administrators to **protect systems, users, and data**.
* There are **three main categories** of security controls:
  + **Physical controls**
  + **Logical (technical) controls**
  + **Managerial (administrative) controls**

**2. Physical Security Controls**

**2.1 Definition and Purpose:**

* Designed to **protect people and facilities** from **real-world physical attacks**.
* Enhance an organization's **physical security posture** by limiting access to **buildings or restricted areas**.

**2.2 Application Areas:**

* Common protected areas include:
  + **Offices**
  + **Communication closets**
  + **Server rooms**

**2.3 Examples:**

* **Fences**, **locks**, and **security badges**
* **Proximity cards** and **access control vestibules**
* **Guards** and **biometric devices**
  + Such as **fingerprint**, **retina**, **facial recognition**, and **palm print scanners**

**3. Logical (Technical) Security Controls**

**3.1 Definition and Purpose:**

* Also known as **technical controls**.
* Implemented using **hardware or software** to prevent/restrict system access.

**3.2 Examples:**

* **Firewalls**, **IDS/IPS**, and **authentication mechanisms**
* **Encryption**, **security protocols**, and **access control lists**
* **Auditing** (point-in-time evaluation)
* **Monitoring** (continuous observation)

**3.3 Clarification: Auditing vs. Monitoring**

* **Auditing**: One-time activity (e.g., penetration test) – verifies current security status.
* **Monitoring**: Ongoing process that ensures **continuous evaluation** of system performance and behavior.

**3.4 Continuous Monitoring Requirements:**

* Necessary for organizations aiming to become more **effective** and **efficient**.
* Includes:
  + **Change management** with baselines
  + **Configuration management**
  + **Automated log collection and triage**
  + **Security system and network analysis**
* Outputs help determine the **effectiveness of current controls** and where improvements are needed.

**4. Managerial (Administrative) Controls**

**4.1 Definition and Purpose:**

* Also known as **administrative controls**.
* Concerned with managing **people and policies**, not technology.
* Implemented through:
  + **Policies**
  + **Procedures**
  + **Guidelines**
  + **Standards**
  + **Baselines**

**4.2 Examples:**

* **Data classification and labeling**
* **Personnel supervision**
* **Security awareness training**

**4.3 Importance of User Training:**

* Training is one of the **most effective administrative controls**.
* It’s also one of the **most cost-effective** security investments.
* Many security incidents could have been prevented with **proper user education**.

**5. Course Focus – Objective 2.1: Security Measures and Their Purposes**

* This section supports **CompTIA A+ 220-1102 Objective 2.1**: Summarize various **security measures** and their **purposes**.
* Topics covered in this course section include:

**5.1 Physical Controls (Detailed Examples):**

* **Fences**
* **Bollards**
* **Lighting systems**
* **Security guards**
* **Video surveillance (CCTV)**
* **Alarm systems**
* **Magnetometers**

**5.2 Physical Access Controls:**

* **Door locks** (mechanical and electronic)
* **PINs and keypads**
* **Smart cards and badge readers**
* **Key fobs**
* **Biometric systems**:
  + Fingerprint, palm, retina, facial recognition, voice recognition

**5.3 Logical Control Principles:**

* **Least privilege**
* **Access control lists (ACLs)**
* **Zero Trust Architecture**

**5.4 Multi-Factor Authentication (MFA):**

* Adds **multiple verification layers**.
* Enhances **logical/technical security** by validating identity using:
  + Something you know (password)
  + Something you have (token)
  + Something you are (biometrics)

**5.5 Device and Mobility Management:**

* **Enterprise Mobility Management (EMM)**
* **Mobile Device Management (MDM)**
* Both are critical in protecting:
  + **Smartphones**
  + **Tablets**
  + **Remote endpoints**

**5.6 Data Loss Prevention (DLP):**

* Prevents **unauthorized access**, **transmission**, or **leakage** of sensitive data.

**5.7 Identity and Access Management (IAM):**

* Controls how users are **identified and authenticated**.
* Key technologies:
  + **SAML (Security Assertion Markup Language)**
  + **Single Sign-On (SSO)**
  + **Just-In-Time Access (JIT)**
  + **Privileged Access Management (PAM)**

**5.8 Active Directory Security Measures:**

* **Domain-based environments**
* **Security groups**
* **Organizational Units (OUs)**
* **Group Policies**
* **Login scripts**
* **Home folder redirection to network shares**

**6. Summary and Next Steps**

* This section provides a foundation in:
  + **Understanding**, **implementing**, and **differentiating** types of security controls.
  + Categorizing them as **physical**, **logical**, or **managerial**.
* Upcoming content continues to explore these control types **in depth**, providing applied examples from enterprise environments.

Would you like a **quiz** tailored to this document and mapped directly to **CompTIA A+ 220-1102 Objective 2.1** for active recall and exam readiness?