Got it! Let’s simplify and clean up the formatting while maintaining clarity and professional structure. I’ve **removed the decimal-style numbering** and restructured it into a **flat, readable bullet format** with numbered major sections only — ideal for **Word pasting** and focused on **CompTIA A+ 220-1102 (Objective 2.1)**.

**Identity and Access Management (IAM) – Study Notes**

**CompTIA A+ 220-1102 | Objective 2.1 – Security Concepts**

**1. What Is IAM?**

* IAM stands for **Identity and Access Management**.
* It ensures that users and devices are:
  + **Identified** (who they are),
  + **Authenticated** (proof of identity),
  + **Authorized** (given permission to access resources).
* Applies to users, computers, applications, and other entities.
* A basic example is logging in with a **username and password**.

**2. Unique Subjects in IAM**

IAM manages identity for different subject types across an organization:

**Personnel (Users):**

* Most common IAM subject.
* Refers to employees or users accessing systems.
* Can pose risk by:
  + Writing down passwords,
  + Mishandling credentials,
  + Being socially engineered.

**Endpoints:**

* Includes desktops, laptops, tablets, smartphones.
* Each device may have **its own IAM identity**.
* Used by personnel to access systems.

**Servers:**

* Serve as back-end systems communicating with other machines.
* Use IAM for secure communication.
* Each server has its **own credentials**.

**Software:**

* Applications and services can act as IAM subjects.
* Access is often controlled via **digital certificates**.
  + Able to allow or disallow a client from doing certain things with a certain piece of software.

**Roles:**

* Represent the **function** or **job title** (e.g., Admin, Finance, Help Desk).
* Used in **group-based access control**.
* Easier to manage permissions by group than by individual.

**3. IAM Components and Functions**

**Technical Components:**

* IAM systems often include:
  + **Directory services** (like Active Directory),
  + **Authentication tools** (passwords, biometrics),
  + **Auditing/reporting tools** for accountability.

**Common IAM Tasks:**

* **Provisioning** – Creating new accounts.
* **Deprovisioning** – Disabling/deleting accounts.
* **Account Management** – Changing passwords or roles.
* **Auditing** – Reviewing logs for unusual activity.
* **Threat Evaluation** – Identifying weak passwords or inactive accounts.
* **Compliance** – Ensuring rules and regulations are followed.

**4. IAM Risk Types**

**User Accounts:**

* Regular user logins for daily tasks.
* Low risk but should be monitored.

**Privileged Accounts:**

* High-level access (admin/root).
* Can make system-wide changes.
* High risk – require tight control and logging.

**Shared Accounts:**

* Used by multiple people under one login.
* Common in home or small office setups.
* Not recommended due to:
  + Lack of user accountability,
  + Poor auditing capability.

Let me know if you'd like a **quiz next** on IAM concepts — I can keep that formatting clean and consistent as well.

Here is a **6-question multiple-choice quiz** based on the *Identity and Access Management Notes*, designed to simulate the style and rigor of the **CompTIA A+ 220-1102 exam (Objective 2.1 – Security Concepts)**. The format is optimized for **Word**, with minimal spacing and clear professional layout.

**Identity and Access Management (IAM) Quiz – CompTIA A+ 220-1102 (Objective 2.1)**

**1.** Which of the following best describes the purpose of Identity and Access Management (IAM)?  
a) To provide data encryption on remote storage systems  
b) To create wireless access points for organizational use  
c) To authenticate users and assign appropriate access to resources  
d) To enforce printer usage quotas in networked environments

**2.** A company uses Active Directory to manage user logins and enforce authentication policies. This is an example of what kind of IAM component?  
a) Role-based policy handler  
b) Digital software validator  
c) Directory service  
d) Remote access gateway

**3.** Which of the following is a security risk associated with shared accounts?  
a) Users receive duplicate access permissions  
b) Updates are performed in real time  
c) Activities cannot be linked to a specific user  
d) They automatically log out inactive sessions

**4.** Which IAM subject type applies to mobile devices such as tablets and smartphones that are used to access company systems?  
a) Software  
b) Endpoints  
c) Roles  
d) Personnel

**5.** An administrator account capable of installing software and changing system settings is an example of what type of IAM account?  
a) Shared account  
b) Software agent  
c) User-level account  
d) Privileged account

**6.** What is the purpose of provisioning in an IAM system?  
a) Reviewing security logs for unauthorized access  
b) Blocking applications from accessing restricted folders  
c) Creating new user accounts with the correct access level  
d) Encrypting all file transfers between endpoints

Once you provide your answers, I’ll return a **fully explained answer key** that is formatted for clean pasting into Word.

Excellent! Here's your **professionally formatted answer key and explanation sheet** for the IAM quiz, aligned with **CompTIA A+ 220-1102 (Objective 2.1 – Security Concepts)** and ready for **clean pasting into Microsoft Word**.

**Answer Key & Explanations – Identity and Access Management (IAM) Quiz**  
**CompTIA A+ 220-1102 | Objective 2.1 – Security Concepts**

**1. Answer: c – Correct**  
**Your Answer: c – Correct**  
**Explanation:**  
IAM is designed to **authenticate users and assign appropriate access** based on roles and identities. It manages who has access to what within an organization’s IT systems.

**2. Answer: c – Correct**  
**Your Answer: c – Correct**  
**Explanation:**  
**Directory services** like **Active Directory** store and manage user account information and enforce authentication rules, making them a core IAM component.

**3. Answer: c – Correct**  
**Your Answer: c – Correct**  
**Explanation:**  
Shared accounts are a **security risk** because activity **cannot be traced** back to a specific user, making **auditing and accountability** very difficult.

**4. Answer: b – Correct**  
**Your Answer: b – Correct**  
**Explanation:**  
**Endpoints** such as laptops, tablets, and smartphones are IAM subjects. Each has unique credentials and interacts with the network, separate from the user’s identity.

**5. Answer: d – Correct**  
**Your Answer: d – Correct**  
**Explanation:**  
**Privileged accounts** include administrator/root/superuser roles and can perform system-critical functions like installing software and managing other users. These are **high-risk accounts**.

**6. Answer: c – Correct**  
**Your Answer: c – Correct**  
**Explanation:**  
**Provisioning** refers to the process of **creating new accounts** and ensuring users receive the correct access rights based on their job function or role.

**✅ Final Score: 6 / 6 – Excellent!**

You've demonstrated full mastery of **IAM roles, account types, and risk awareness** — all crucial knowledge for passing the **CompTIA A+ 220-1102 exam**.

Would you like a follow-up quiz combining IAM, DLP, and MFA topics for review depth?