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.