Below is the **sentence-by-sentence analysis** of the *“Data Loss Prevention Notes”* document, converted into **professionally formatted study notes**. The structure is optimized for **CompTIA A+ 220-1102 exam preparation** under **Objective 2.1 (Security Concepts)** and formatted for **clean pasting into Microsoft Word** — minimal spacing, aligned paragraphing, and clear numbering.

**Data Loss Prevention (DLP) – Study Notes**

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

**1. Purpose and Definition of DLP**

* **1.1** Data Loss Prevention (DLP) is a **software-based solution** designed to detect and prevent **sensitive data** from:
  + Being **stored on unauthorized systems**
  + Being **transmitted over unauthorized networks**
* **1.2** DLP aims to **keep data under organizational control** and prevent it from leaving the network environment.

**2. Key Components of a DLP System**

* **2.1 Policy Server:**
  + Central hub for **configuring DLP rules**, such as:
    - Data **classification**
    - **Confidentiality** rules
    - **Privacy policies**
  + Defines how incidents are **logged and reported**
* **2.2 Endpoint Agent: Enforce policy on client computers, even offline.**
  + Installed on **client devices** (e.g., laptops)
  + Enforces policy **even when disconnected** from the network
  + Example: Prevents file transfer to external drives when offline
* **2.3 Network Agent:**
  + Functions as a **network appliance**
  + Sits at the **network boundary** to:
    - Intercept traffic (e.g., email, web)
    - **Scan messages**
    - **Block data exfiltration**

**3. Data Format Types Scanned by DLP**

* **3.1 Structured Data:**
  + Organized and formatted in predictable ways
  + Examples: **JSON files**, **CSV spreadsheets**
  + Fields are predefined and follow a strict schema
* **3.2 Unstructured Data:**
  + Freely formatted information
  + Examples: **Emails**, **Word documents**, **chat messages**

**4. Policy Enforcement in Data Transfer**

* **4.1** DLP systems monitor file transfers and **block actions** that **violate policy**.
* **4.2** Transfers are analyzed **against preset rules**, and **actions are triggered** if violations occur.

**5. Real-World Interface and Monitoring**

* **5.1** Most DLP systems include a **dashboard** that shows:
  + **Policy matches**
  + **False positive rates**
  + Ability to **create or update policies**
* **5.2** Example: Microsoft’s DLP feature in **Office 365** provides centralized monitoring.

**6. DLP Remediation Actions**

There are **four levels of DLP response**, depending on policy settings:

**6.1 Alert:**

* **Allows the user action**, but logs the violation
* Admin receives a report (e.g., copying a file to a USB is allowed but flagged)

**6.2 Block:**

* Prevents the **action from occurring** (e.g., blocks copying to USB)
* File remains **accessible** within the system, but **cannot be exported**

**6.3 Quarantine:**

* File becomes **inaccessible** to the user or others
* Often includes **encrypting the file** to prevent access
* Triggered by high-sensitivity data violations

**6.4 Tombstone:**

* Replaces the original file with a **notice** file
* Message explains that the file has been removed due to **DLP policy violation**
* May include **instructions** for restoring access

**7. DLP Remediation Locations**

* **7.1 Client-Side:**
  + Handled by **endpoint agents** on user devices
* **7.2 Server-Side:**
  + If the server has a DLP agent installed
* **7.3 Network Boundary:**
  + Via **network appliances** scanning outgoing data traffic

**8. Exam Considerations**

* **8.1** The **CompTIA A+ 220-1102 exam** does **not** test DLP configuration.
* **8.2** You are expected to understand:
  + The **purpose** of DLP
  + How DLP **functions**
  + What types of **remediation** exist
  + Where DLP enforcement can occur