Absolutely! Below is a **comprehensive sentence-by-sentence breakdown** of the document **“116. FileVault.docx”**, rewritten into deeply detailed **study notes** for the **CompTIA A+ 220-1102 exam**. This falls under **Objective 1.8**, which covers macOS features, including **disk encryption technologies like FileVault**.

**🧠 Study Notes – FileVault (macOS Full Disk Encryption)**

**🔐 What Is FileVault?**

* **FileVault** is a **full disk encryption tool** built into **macOS**.
* Its purpose is to **encrypt all data stored** on a hard drive (HDD) or solid-state drive (SSD).
* This protects data from being **read or accessed by unauthorized users**, especially in case of **device theft or loss**.

**🚨 Why Is FileVault Important?**

* If a **threat actor** physically takes your Mac, FileVault **prevents them from reading your files**.
* The system requires **decryption on every boot**, using a **secure shared secret** (your password).
* Without the password, data on the drive remains **completely inaccessible**.

**🧑‍💻 How Does FileVault Work?**

* When FileVault is enabled:
  + It encrypts the disk contents using strong algorithms.
  + Decryption only happens **after login**, using:
    - A **user-defined password**, or
    - A **recovery key**, or
    - An **iCloud account**, if configured

**🛠️ How to Access FileVault Settings**

**Two Ways to Open It:**

1. **System Preferences > Security & Privacy > FileVault**
2. Press Command + Space to open **Spotlight** → Type **“FileVault”** → Hit Enter

**Once inside:**

* The **FileVault tab** will be selected automatically.
* It will show whether FileVault is **On or Off**.

**🔓 Turning Off FileVault**

1. Click the **lock icon** to unlock changes.
2. Enter your **administrator credentials**.
3. Once unlocked, click **“Turn Off FileVault”**.
4. You’ll be asked **“Are you sure?”** → Click **Yes**.
5. Re-enter your password to confirm.
6. FileVault begins the **decryption process**, and encryption is removed from the disk.

**🔐 Turning On FileVault**

1. Go to **System Preferences > Security & Privacy > FileVault**.
2. Click **Turn On FileVault**.
3. You’ll be prompted to **choose a recovery method**:
   * Use your **iCloud account**
   * OR
   * **Generate a recovery key**
     + If using a recovery key:
       - A unique code will appear on screen.
       - **Store this code safely!** It’s essential for recovery if you forget your password.
       - If both the password and recovery key are lost, **all encrypted data will be permanently lost**.

**⚙️ Encryption Process**

* After setup:
  + Click **Continue** to start encryption.
  + macOS will begin encrypting your system drive (Mac HD).

**⏱️ Time It Takes:**

* Varies based on drive type:
  + **SSD (Solid-State Drive)**: ~30–60 seconds
  + **HDD (Hard Disk Drive)**: ~3–5 minutes

✔ Once complete, a message confirms:

**“FileVault is turned on for disk Mac HD”**

**💾 What Is Data at Rest?**

* Data that is **stored on disk** (not actively in use or in transit).
* FileVault protects **data at rest** from unauthorized access.

**🧪 Real-World Benefits of FileVault**

* If your Mac is **lost or stolen**, and FileVault is enabled:
  + Your personal data remains **inaccessible to attackers**.
  + Without the correct password or recovery key, the encrypted drive is essentially **useless** to others.

**✅ Summary – Key Points for the Exam**

| **Feature** | **Description** |
| --- | --- |
| **FileVault** | Full disk encryption tool for macOS |
| **Purpose** | Protects data from unauthorized access, especially if the device is stolen |
| **Encryption Type** | Data-at-rest encryption using a password or recovery key |
| **Access Location** | System Preferences > Security & Privacy > FileVault |
| **Enable Method** | Click Turn On, choose recovery option (iCloud or recovery key) |
| **Recovery Options** | iCloud, recovery key (store securely!) |
| **Login Requirement** | Password required at boot to decrypt and access files |
| **Disabling** | Requires admin credentials and confirmation |
| **Decryption Time** | SSD = 30–60s, HDD = 3–5 mins |
| **Security Note** | Losing both the password and recovery key results in **total data loss** |
| **Data at Rest** | FileVault protects stored (inactive) data |

**🎯 CompTIA A+ 220-1102 Relevance**

* **Objective 1.8:** Identify common macOS tools and their purpose
* Expect to be asked:
  + What FileVault does
  + Where it is located
  + What happens if both recovery key and password are lost

✔ No need to perform setup—just recognize its function and importance.