Below is a **detailed, sentence-by-sentence analysis** of the document titled **“220. Encrypting Windows Devices Notes”** presented in **clean, professional study note format** for seamless copy-pasting into Microsoft Word. This format is built for **CompTIA A+ 220-1102 Objective 2.5** compliance and leaves no key detail omitted.

**Encrypting Windows Devices – Study Notes**

**(CompTIA A+ 220-1102 – Objective 2.5)**

**1. Overview of Encryption Options in Windows**

* Windows supports **three main encryption methods**:
  1. **Encrypting File System (EFS)**
  2. **BitLocker**
  3. **BitLocker To Go**

**2. Encrypting File System (EFS)**

* **EFS** is a feature of the **NTFS file system** that supports **file and folder encryption**.
* EFS is **not available** in Windows Home edition.
  + Only supported in **Windows Pro, Education, and Enterprise** editions.
* Designed to encrypt **data at rest**, which refers to:
  + Data stored on HDDs, SSDs, or USB thumb drives.
* Encryption is not applied to:
  + **Data in use** (actively processed in memory)
  + **Data in transit** (moving across a network)

**2.1 Protecting Data**

* **Data at rest**: Stored but not in use (e.g., files on disk).
* **Data in use**: Actively processed in memory/CPU.
* **Data in transit**: Moving over a network; protected using **SSL/TLS encryption**.
  + **Creating secure tunnels from clients to destination**.

**2.2 EFS Encryption Process**

* Right-click on a file/folder → **Properties** → **Advanced**.
* Under Advanced Attributes:
  + Check **“Encrypt contents to secure data”**.
  + Apply and confirm changes.
* Encrypted files/folders appear **with green text labels** in File Explorer.
* **Only the user account that encrypted the file** can decrypt it.

**2.3 EFS Limitations**

* **Tied to the user account’s password**.
  + If compromised, all EFS-protected data becomes vulnerable.
* **Selective encryption**:
  + Only encrypts specific files/folders.
  + Must be manually applied to each item.
* **Not ideal for full-system encryption** or protecting large quantities of data.

**3. BitLocker – Full Disk Encryption**

* **BitLocker** is a **full disk encryption** feature in Windows.
* Not available in **Windows Home**.
  + Supported in **Windows Pro, Education, and Enterprise**.
* Encrypts **entire drives** automatically:
  + All files and folders are protected without needing manual selection.
* Requires the user to set up a **long, strong password** for encryption.

**3.1 BitLocker Drive Compatibility**

* BitLocker supports **internal drives only**:
  + HDDs and SSDs that are permanently installed.
* Does **not support** external/removable media:
  + E.g., USB flash drives or portable HDDs.

**4. BitLocker To Go – Encryption for Removable Media**

* Companion to BitLocker, used for **removable data drives**.
* Supports:
  + USB flash drives
  + SD cards
  + External HDDs
* Compatible with drives using **NTFS, FAT32, or exFAT** file systems.

**4.1 BitLocker To Go Encryption & Access**

* Drive is encrypted using:
  + **Password**
  + Or **Smart card/token**
* To decrypt on another system:
  + Users must supply the **same password or smart card**.
* Useful for ensuring portable data remains encrypted and secure.

**5. Choosing the Right Encryption Method**

| **Scenario** | **Recommended Encryption Method** |
| --- | --- |
| Encrypt individual files/folders | **EFS** |
| Encrypt internal fixed drives (HDD/SSD) | **BitLocker** |
| Encrypt removable drives (USB, SD cards) | **BitLocker To Go** |

* All options require NTFS or compatible file systems.
* All options are **not supported** on **Windows Home edition**.

**6. Summary of Encryption Use Cases**

* **EFS**: Ideal for **specific files/folders** on NTFS-formatted internal drives.
* **BitLocker**: Best for **full internal drive encryption**, protecting all data at rest.
* **BitLocker To Go**: Designed for **removable drive encryption**, with secure access via password or smart card.

**Real-World Use Cases**

* **Small Business Laptop Protection**:
  + An organization uses **BitLocker** to encrypt employee laptops. If stolen, all data remains protected.
* **Contractor Working with Sensitive Data**:
  + A freelancer encrypts project folders with **EFS** to isolate and protect specific client files.
* **Field Technicians Using USB Drives**:
  + Field workers use **BitLocker To Go** to secure USB drives containing configuration tools and customer data.