Here’s the **comprehensive sentence-by-sentence study note breakdown** of your *“Documentation Types Notes”* document, formatted professionally for Word, numbered for clarity, and retaining all critical details.

**Documentation Types – Study Notes**

1. **Overview of Documentation Types for Technicians**
   * Common types:
     + **Acceptable Use Policies (AUP)**
     + **Standard Operating Procedures (SOPs)**
     + **Incident Reports**
     + **Network Topology Diagrams**
2. **Acceptable Use Policies (AUP)**
   * Define what employees **can and cannot do** with company services or resources.
   * Enforced by the organization to govern its employees and users.
   * Tailored to organizational values and workflows; no universal standard.
   * Examples:
     + Religious organization → Block gambling/porn sites.
     + Casino → Allow gambling site access for competitive research.
     + Playboy → Allow adult site access for industry purposes.
   * US Government example: No gambling, pornography, or online buying/selling on work computers (e.g., eBay, Craigslist).
   * Restrictions may apply to:
     + Websites visited.
     + Applications installed.
     + Phone calls made (e.g., block personal long-distance calls).
   * May include **regulatory compliance** clauses:
     + Monitoring all activity on company devices/networks.
     + Logging and reporting user actions (e.g., bank logins, social media use).
   * **Splash screens** may be used to reinforce AUP:
     + Shows up when someone tries to log into a computer.
     + Displayed before login (Windows 10/11).
     + Include a small paragraph with text, legal statements binding user to AUP upon clicking “OK.”
     + Example: Department of Defense systems require explicit acknowledgment of terms.
       1. For example, anytime you log into a department of defense computer in the US government network, it will state that you are accessing aa US government information system. That is provided for us GOVERNMENT AUTHORIZED use only.
          1. By using this information system which includes any devices attached to this information system you consent to the following terms, and it has a list of things that you’re consenting to.
          2. Once you click Ok you will agree with the terms.
          3. The organization will hold it against you any time you break the terms of this acceptable use policy.
   * Violating the AUP can result in enforcement actions.
3. **Standard Operating Procedures (SOPs)**
   * Step-by-step actions to ensure consistent execution of tasks in compliance with policy.
   * For example: There are a lot of different ways to give somebody access rights to a particular file or folder on a system.
     + Your organization may use security groups to do that.
     + Others use discretionary access controls and applies those rights to the individual user on the folder.
   * Goal: All employees follow **the same method** for specific actions.
   * Examples of SOPs:
     + New user setup checklist.
     + End-user termination checklist.
     + Software installation procedures.
   * SOP content often includes text plus visual aids (screenshots, videos).
   * **New User Setup SOP**:
     + For example, a new user setup checklist and procedure can have a SOP for new employees when they get hired, which can include:
       1. Issuing ID badge, secure credentials, device issuance, security group assignment, office location, system login instructions.
   * **End-User Termination SOP**:
     + For example, whenever an employee leaves the company you have a set of things that need to be done as well to offboard that employee properly.
     + We call this the end-user termination checklist and procedures, or the end-user standard operating procedure.
     + The standard operating procedure can include:
       1. Return/sanitize devices, release software licenses, disable accounts, reclaim ID badge, change shared passwords/locks.
   * **Software Installation SOP**:
     + Verify system requirements, confirm authentic download source, check file hash, validate license, install software, follow change control/monitoring, train end-user.
   * Even small companies may have dozens of SOPs (e.g., Dion Training has 50+).
4. **Incident Reports (After Action Reports / Lessons Learned)**
   * Purpose: Document details of major incidents to **learn from and prevent recurrence**.
   * Completed after incident resolution.
   * Collects input from: Users, customers, technicians, managers, stakeholders.
   * Key elements:
     + What happened.
     + What caused it.
     + How to prevent it in the future.
   * Example: Web server crash investigation → Determine cause (overload, power loss, hardware failure, network outage) → Implement preventative measures.
   * Reports should be **widely shared internally** to promote organizational learning.
     + Make sure these are widely published across our organization so that other people can learn from our mistakes and understand what the underlying causes were and how we can implements preventative measures to prevent this from happening in the future.
5. **Network Topology Diagrams**
   * Show network design and device connectivity.
   * **Two types**: Logical and Physical diagrams.
   * **Logical Diagram**:
     + Focus on Layer 2/Layer 3 (data flow, IP schemes, port connections).
     + Useful for diagnosing connectivity and routing issues.
   * **Physical Diagram**:
     + Focus on Layer 1 (physical layout, cabling, device locations).
     + Often overlaid on building floor plans.
     + Shows routers, switches, cable runs, and physical infrastructure.
   * Scale varies by network size:
     + Small networks: May include all endpoints.
     + Large networks: Show only core routers/switches and edge switches; details broken out in sub-diagrams if needed.
   * Choosing diagram type depends on troubleshooting layer:
     + Layer 2/3 issues → Logical diagram.
     + Layer 1 issues → Physical diagram.
6. **Key Takeaway**
   * Technicians should be familiar with:
7. **AUPs** – Define and enforce acceptable resource use.
8. **SOPs** – Ensure consistent, documented task execution.
9. **Incident Reports** – Capture lessons learned from outages.
10. **Network Topology Diagrams** – Provide visual network structure for troubleshooting.