**3) Law\_Enforcement\_SOC\_Policy\_Framework.docx**

**Security Policy Framework – Law Enforcement SOC Simulation Project**

**Purpose:** provide concise rules for the way you operate your Wazuh-based SOC lab so your submission meets governance requirements.

**1. Access Control Policy**

* Use a dedicated analyst account on Windows; restrict admin use to when needed.
* Protect Wazuh Dashboard credentials; change defaults and store securely.
* Limit roles in Dashboard (viewer vs. admin) to least privilege.
* Lock the screen when away; sign out after work sessions.

**2. Data Protection Policy**

* Store logs inside Docker volumes (default Wazuh stack).
* Keep configuration files (e.g., /var/ossec/etc/ossec.conf) accessible only to admin/root.
* Transmit agent→manager over the standard Wazuh channels; preserve certs used by the stack.
* Save all screenshots/evidence in a versioned folder for the course.

**3. System Use Policy**

* Only run **authorized** test actions on Ubuntu/Parrot OS as part of this lab.
* No real-world exploitation; keep everything inside your local lab.
* Keep Ubuntu updated:
* sudo apt update && sudo apt upgrade -y
* Document changes (what/why) in Monday.com day comments.

**4. Governance & Roles**

| **Role** | **Responsibility** |
| --- | --- |
| SOC Analyst (you) | Daily alert review, agent health checks, evidence capture, day comments. |
| Instructor / Reviewer | Reviews screenshots/docs; signs off rubric items; suggests improvements. |
| System Admin (lab owner) | Maintains Docker/Wazuh services and OS updates on host. |

**References used in this project:** Wazuh SIEM stack, MITRE ATT&CK matrix (as displayed in your dashboard), CIS Ubuntu 22.04 benchmark results.