ISO 27001-aligned policy trio - Access, Logging, Vulnerability

Day 3 – ISO 27001:2022 & Policies

Mini Project
Week 6.3

15th of *October, 2025*

Lead: *Muhammad Tayyab*
Athar Imran (Buildables Cybersecurity Fellow)

Access Control Policy:

- A.8.2 Identity Management
- A.8.3 Access Control
- A.5.17 Authentication Information
- A.5.18 Privileged Access Rights

- All users must have an ID number with an individual assigned.
- Documentation must be made for access granting and revoking access.
- Default credentials be made prohibatae
- MFA must be imposed; no compromise for privileged accounts.
- Access rights must be reviewed regularly.
- Failed access attempts and privilege escalation must be monitored.

Logging Policy:

- A.8.15 Logging
- A.8.16 Monitoring Activities
- A.8.18 Clock

- Authentication, system changes, security events, and network activities must be logged.
- Log forwarding be made real-time.

- ➔ Log retention period should be defined. Min 1 year.
- ➔ Log be made tamper-protected and only visible to SOC & audit team.
- ➔ Multiple failed logins, privilege escalation, data exfiltration, or anomalous behaviors must generate an alert.
- ➔ Daily review & track recording is a must for SOC.

Vulnerability Management Policy:

- ❖ A.8.23 Technical Vulnerability Management
- ❖ A.8.9 Configuration Management
- ❖ A.8.13 Backup

- ➔ Monthly or after a major change, vulnerability scanning must be conducted.
- ➔ CVSS must be labeled to identified vulnerabilities.
- ➔ Remediation must be done within:
  - ◆ Critical: within **72 hours**
  - ◆ High: within **7 days**
  - ◆ Medium: within **30 days**
  - ◆ Low: within **90 days**
- ➔ Patch deployment must be tested and documented.
- ➔ Correlation of vulnerability data with threat intelligence feeds must be achieved to identify active exploitation trends.