Baseline User & Group Policy — Linux IAM & Server Hardening
Student: Sanjana Thawait (ERP ID: 6604710)

Objective:
Implement secure Identity & Access Management on Ubuntu using:
- Users, Groups, Sudo (least privilege)
- POSIX Permissions + ACL
- AuditD logging to track privileged file changes

Roles:
Admins (group: admins)
- Full sudo privileges
- System configuration

Developers (group: devs)
- Limited sudo access (only specific commands)
- No unrestricted sudo

Auditors (group: auditors)
- Read-only access to logs
- No write/execute on system config

Shared Folder (/srv/project):
- Owner: root
- Group: project
- ACL: developers = read/write, auditors = read-only

Audit Rules (auditd):
- Monitor changes to /etc/sudoers & /etc/passwd