PROJECT REPORT: AI Biosecurity Compliance Auditor

Team Name: BioSec | **Track:** Track 3 – AI Biosecurity Tools

1. Executive Summary

Traditional biosecurity relies on static, manual checklists that create a dangerous implementation gap. Our system, the **AI Biosecurity Compliance Auditor**, bridges this gap by transforming high-level policies into enforceable, real-time lab protocols. By combining computer vision with heuristic risk scoring, we enable labs to move from reactive box-checking to proactive, auditable defense. [2, 3, 4]

2. Problem Statement

- **Static Policies:** Regulations like the Denver Biosecurity Framework are often buried in PDFs, making them difficult to operationalize at the bench.
- **Human Error:** Minor slips (e.g., improper PPE) can escalate into systemic incidents, yet real-time monitoring is currently non-existent in most labs. [5, 6, 7]

3. The Solution: Three-Layer Risk Engine

1. **Policy-to-Protocol Mapping:** Uses an LLM to ingest regulatory frameworks and automatically generate step-by-step Standard Operating Procedures (SOPs) tailored to specific lab equipment.
2. **Real-Time Auditing (Computer Vision):** Continuous monitoring of safety practices (PPE compliance, door security) using edge-AI to detect "Critical Fails" instantly.
3. **Consequence Modeling (Violation Simulations):** A heuristic model that runs "What If" simulations to show how specific compliance failures increase the mathematical probability of a biosecurity incident. [6, 8, 9, 10, 11]

4. Technical Architecture

- **Data Acquisition:** Integration of structured lab inputs and live video feeds.
- **Analytical Layer:** Custom heuristic risk scoring that aggregates compliance data into a live "Lab Safety Heatmap".
- **Decision Support:** Automated reporting for regulators and instant alerts for lab personnel. [9, 10, 12, 13]

5. Impact & Future Vision

This platform establishes an **auditable workflow** for the AI-driven biology era, enabling regulators to verify safety without constant physical inspections. Future iterations will include DNA synthesis screening logic to flag high-risk orders alongside safety protocols. [7, 14, 15]