Aegis-AI Models + Backend Guide

For 2 members: feasibility, ML reasoning, deployment plan, tough Q&A

1. Model/Backend Team Mission

Your job: prove feasibility and technical seriousness. Mentors want to know you understand the ML problem, constraints (offline), and deployment plan.

- Explain what signals matter (pitch jitter, spectral artifacts, vocoder traces, temporal consistency).
- Explain how you would train (ASVspoof, etc.) and evaluate (EER, ROC-AUC).
- Explain deployment: quantization, ONNX/TFLite, edge runtime.
- Explain security: secure storage, logs, tamper resistance.

2. Demo behavior (localhost)

The localhost demo shows the end-to-end product behavior: upload → analysis → forensic report. It's optimized for speed and presentation.

- audio1/audio3 represent authentic examples.
- audio2/audio4 represent synthetic examples.
- Reports vary per file (IDs, metrics, anomaly scores, graphs) to reflect real-world differences.

3. RunAnywhere SDK (deeper talking points)

- We need predictable, fast inference on edge hardware.
- RunAnywhere helps packaging and running optimized models on-device.
- We will ship quantized models; inference happens locally.
- Optional federated learning: share model updates, not raw media.

4. Hard technical questions you may get

- Q: How do you handle noisy audio? A: VAD + robust features; confidence thresholding; recommend re-capture.
- Q: Can attackers bypass? A: We use multiple signals + continuous model updates; also operational policies.
- Q: Why not cloud? A: Field settings often have no internet; privacy/security constraints.
- Q: What metrics prove accuracy? A: EER, ROC-AUC, precision/recall at operating points.
- Q: How do you scale adoption? A: pilots with agencies, per-device licensing, training + SOP integration.