TECHNICAL ROUND INSTRUCTIONS – AI/ML Internship

Fenrir Security Private Limited
Date Issued: *17 June 2025*

1 · TASK OBJECTIVE

Build a mini end-to-end demo that:

A. **Data Prep** – Gather ≥ 150 public Q&A pairs on command-line topics (Git, Bash, tar/gzip, grep, venv, …).

B. **Model Fine-Tuning** – Choose any open-weights model ≤ 2 B parameters (e.g., TinyLlama-1.1B, Phi-2) and fine-tune it with LoRA/QLoRA for one epoch on free Colab T4 or local GPU.

C. **CLI Agent** – Wrap the resulting adapter in a agent.py script that:
   - Accepts a natural-language instruction from the terminal.
   - Generates a step-by-step plan with the fine-tuned model.
   - If the first line looks like a shell command, execute it in dry-run mode (echo <cmd>).
   - Logs each step to logs/trace.jsonl.

D. **Static & Dynamic Evaluation** – Compare base vs. fine-tuned outputs on the five test prompts in §7 and two extra edge-cases you design; compute a simple metric (BLEU / ROUGE-L) and score plan quality (0-2).

E. **Report** – One-page report.md covering data sources, hyper-parameters, training cost/ time, evaluation results, and two improvement ideas.

2 · TIMELINE & DEADLINE

- **Clock starts:** When you receive this email.
- **Duration:** 24 hours.
- **Hard deadline:** 10 PM IST, Wednesday 18 June 2025.
- **Extensions:** None; delays without prior written approval disqualify the submission.

3 · REQUIRED DELIVERABLES

- Source & build instructions (README.md)—end-to-end reproducible.
- data/ – JSON file(s) containing ≥ 150 validated Q&A pairs.
- Training notebook / script and LoRA adapter files (≤ 500 MB).
- agent.py – Runnable as:python agent.py "Create a new Git branch and switch to it"
- eval_static.md – Base vs. fine-tuned answers + metrics.
- eval_dynamic.md – Agent runs + 0-2 scoring table.
- report.md – One-page summary.
- Demo video (≤ 5 min, Loom/MP4).

4 · SUBMISSION GUIDELINES

- Do NOT share repositories or public links.
- Email all deliverables (or a private access-restricted link) to hr@fenrir-security.com using the subject line:
"AI/ML Internship Technical Task Submission – ".
- Ensure the email timestamp is on or before the deadline.

5 · CONFIDENTIALITY & INTEGRITY

- All task materials and deliverables are the exclusive property of Fenrir Security Private Limited.
- Do not publish, open-source, or discuss any part of this challenge publicly.
- We may run plagiarism and licence-compliance checks or request a live walkthrough (Round 2) before final evaluation.

6 · DISQUALIFICATION CRITERIA

- Late submission without written approval.
- Missing or non-functional deliverables.
- Public disclosure of task details or outputs.
- Use of proprietary/commercial APIs or code without proper licence.
- Failing Round 2 verification (if invoked).