Open-Source Compliance Report

(License Risk, Copyleft Exposure, Remediation Readiness)

---

1. Purpose & Scope

هدف این سند:

- شفاف‌سازی **تمام وابستگی‌های Open-Source**
- شناسایی **ریسک‌های لایسنس) به‌ویژه (Copyleft**
- پاسخ صریح به سؤال حیاتی:

»آیا استفاده از OSS باعث می‌شود محصول مجبور به Open-Source شدن شود یا خیر؟«

این سند شامل:

- کد
- کتابخانه‌ها
- ابزارها
- مدل‌ها
- دیتاست‌ها

---

2. Compliance Principles & Policy

اصول حاکم:

- **No Viral License in Production**
- **No Unknown License**
- **No Transitive Blind Spot**

Policy داخلی:

- بررسی لایسنس قبل از اضافه شدن dependency
- ثبت همه وابستگی‌ها در SBOM
- تأیید Legal/Tech Lead برای هر Copyleft

نبود policy = ریسک انباشته پنهان

---

3. Methodology & Tools Used

روش شناسایی:

- Static dependency scan
- Transitive dependency resolution

- Manual reviewبرای موارد مشکوک

ابزارها:

- license-checker
- pip-licenses
- FOSSA / Snyk / OSS Review Toolkit (در صورت وجود)
- بررسی دستیLICENSE files

صرف «دانستن» کافی نیست؛ باید روش مستند باشد

---

4. Dependency Inventory Overview

Category	Count
Direct dependencies	XX
Transitive dependencies	XXX
OSS libraries	XXX
Proprietary	X

این جدول دید کلی می‌دهد؛ جزئیات جلوتر می‌آید

---

5. License Classification

License Buckets

Permissive (Low Risk)

- MIT
- BSD
- Apache 2.0

Weak Copyleft (Medium Risk)

- LGPL
- MPL

Strong Copyleft (High Risk)

- GPL
- AGPL

این تفکیک زبان مشترک Legal و Tech است

---

6. High-Risk Copyleft Analysis (GPL / AGPL)

Identified Licenses

Dependency	License	Usage Context	Risk
X	AGPL-3.0	Server-side	High
Y	GPL-2.0	Build tool	Medium

Exposure Analysis

- AGPL triggers on **network use**
- GPL triggers on **distribution**

اینجا دقیقاً همان جایی است که سرمایه‌گذار مکث می‌کند

---

7. Product Open-Source Obligation Assessment

Key Question:

Does any license force the product to be open-sourced?

Conclusion:

- No current obligation to open-source core product
- ⚠ One AGPL dependency isolated behind service boundary

پاسخ باید صریح و غیرمبهم باشد

---

8. Mitigation & Cleanup Plan

Actions Defined:

- Replace AGPL dependency with permissive alternative
- Isolate LGPL via dynamic linking
- Document exceptions (if any)

Timeline:

- Short-term (0–30 days)
- Mid-term (30–90 days)

»می‌دانیم ریسک هست» کافی نیست؛ برنامه می‌خواهند

---

9. Transitive Dependency Risk

Findings:

- XX% dependencies are transitive
- Y dependencies have unclear license metadata

Mitigation:

- Lock versions
- Manual license verification
- Dependency pruning

ریسک واقعی اغلب اینجاست، نه درdirect deps

---

10. Open-Source Attribution & Notice Compliance

Current Status:

- License texts stored
- Attribution page planned / implemented
- No missing notices detected

عدم رعایتattribution = breach contract

---

11. ML Models & Data License Compliance

Models

- Base models: Apache / MIT
- Fine-tuning data: owned / licensed

Datasets

- No restricted or non-commercial datasets
- No “research-only” leakage into production

این بخش برای AI سرمایه‌گذاران حیاتی است

---

12. Third-Party API & SDK Usage

Provider	License / ToS	Risk
X	Commercial	Low
Y	Usage-based	Medium

API Terms هم IP risk هستند

---

13. Governance & Ongoing Compliance

Ownership

- OSS Compliance Owner: [Role]

Process

- Quarterly review
- CI license scan
- Dependency approval checklist

بدونprocess ، ریسک دوباره برمی‌گردد

---

14. Known Gaps & Disclosure

Gaps:

- One dependency pending license clarification

Disclosure:

- Fully disclosed
- No known legal claim or notice received

صداقت کنترل‌شده <سورپرایزDD

---

15. Investor Assurance Statement

»بر اساس بررسی‌های انجام‌شده،
هیچ وابستگی Open-Source فعلی
شرکت را ملزم به Open-Source کردن
محصول یا افشای IP نمی‌کند«.

این جمله دقیقاً همان چیزی است که Legal Fund می‌خواهد