AI Compliance Overview – SentinelX / SentinelStack AB

# 1. Syfte

Detta dokument sammanfattar SentinelStacks strategi för att uppfylla kraven i den europeiska AI-förordningen (AI Act 2026), med särskilt fokus på SentinelX-plattformens komponenter, risknivå och säkerhetsåtgärder.

# 2. Systemöversikt

SentinelX är en AI-baserad säkerhetsplattform bestående av:  
- GuardianAgent (Android, on-device NLP)  
- SentinelControlKit (CLI-agent för Windows/Linux)  
- TelegramPanel (för fjärrstyrning och notifiering)  
- PDF-rapportering (WeasyPrint)  
  
Systemet är modulärt, körs lokalt ('local-first') och är designat för att fungera utan moln.

# 3. Riskklassificering enligt AI Act

- Potentiellt high-risk enligt Annex III (2.e): Biometrisk identifikation & sårbara grupper (barn, äldre)  
- SentinelX behandlar inte biometriska data men agerar inom barnskydd  
- Riskreducering sker via full lokal hantering, transparens, användarkontroll och frånvaron av molnintegration

# 4. Säkerhetsåtgärder

- Lokal datalagring och loggning  
- Full manuell kontroll av användare över aktivering/stopp  
- Ingen tredjepartsöverföring utan uttryckligt samtycke  
- Kodsignering och PDF-tidsstämpling  
- Automatisk fallback vid systemfel

# 5. Dokumentation och transparens

Systemet dokumenteras enligt Artikel 13–15:  
- Manualer för användare och administratörer  
- Offentliggörande av AI-modellernas kapacitet och begränsningar  
- Information om risker, säkerhetsrutiner och dataskyddsstruktur  
- Möjlighet till granskning av CLI-källkod (open source-delar)

# 6. Kontakt

Ansvarig organisation: SentinelStack AB  
Kontakt: info@sentinelstack.tech  
Compliance-ansvarig: [Fyll i vid etablering av bolag]