Loggnings- och granskningspolicy – SentinelStack AI Compliance Suite

Denna policy dokumenterar hur loggning, export och granskning av AI-systemens aktiviteter sker enligt AI-förordningen Artikel 12.

# 1. Syfte med loggning

- Bevisa att AI-systemet agerat enligt sin dokumentation  
- Möjliggöra granskning vid incidenter, fel eller extern revision  
- Spåra input, output och beslut som påverkar användare

# 2. Vad loggas?

- Tidpunkt för input/output  
- AI-beslut och rekommendationer  
- Användarkommando (t.ex. fjärrstyrning, overrides)  
- Felhändelser och fallback-aktiveringar  
- Versionshistorik av AI-modell

# 3. Lagringsstrategi

- Loggar sparas lokalt på enhet eller server i krypterad mapp  
- Automatisk rensning efter X dagar (valbart)  
- Manuellt CLI-kommando för radering eller export

# 4. Export och rapporter

- Logg kan exporteras till PDF via CLI (signerad & tidsstämplad)  
- Kan skickas automatiskt till angiven e-post/mottagare  
- Exempelformat:  
 `/logs/events.log`  
 `/exports/log\_report\_2025-06-10.pdf`

# 5. Tillgång till loggar

- Endast auktoriserade användare kan komma åt loggar  
- Systemet använder Telegram-ID whitelist eller lokal inloggning  
- Inga loggar skickas till tredje part utan aktivt godkännande

# 6. Revision och granskningsstöd

- CLI-kommandon för sammanställning:  
 `sentinelstack audit generate`  
- Paket inkluderar:  
 AI-beslut, metadata, användarkommandon, PDF-rapporter

# 7. Efterlevnad AI Act Artikel 12

- Loggning är aktiverad som standard  
- Exporten är tydlig, strukturerad och verifierbar  
- SentinelStack CLI är designat för spårbarhet i alla händelser