Secrets-Policy (Rico 4.5 Genius)

🔐 Sicherheitsrichtlinien

- **Echte Keys NUR in** `.env.local` eintragen (lokal, privat)
- `.env.local` **überschreibt** `.env` - alle Services verwenden diese Priorität
- `.env.local` **ist per** `.gitignore` **ausgeschlossen** und in `.cursorrules` gesperrt
- **In CI/GitHub** werden Secrets ausschließlich über Actions-Secrets injiziert
- **Niemals Secret-Werte loggen** - nur “OK/N/A/Fehler” Status ausgeben

🛡️ Implementierte Sicherheitsmaßnahmen

Environment-Variable Priorität

```
# Alle Services verwenden diese Reihenfolge:
if os.path.exists(".env.local"):
    load_dotenv(".env.local")
load_dotenv(".env")
```

Fehlerbehandlung ohne Key-Leaks

- Einheitliches Mapping: `auth`, `rate_limit`, `server`, `timeout`
- Keine internen Tracebacks in Logs
- Health-Check zeigt nur Status, keine Keys

Git-Sicherheit

```
.env
.env.local
*.env.local
.env.*.local
```

🔑 API-Keys Konfiguration

Erforderliche Keys (in `.env.local`):

```
# OpenAI
OPENAI_API_KEY=sk-...
OPENAI_MODEL=gpt-4o-mini

# Claude (Anthropic)
CLAUDE_API_KEY=sk-ant-...
CLAUDE_MODEL=claude-3-7-sonnet-20250219

# Perplexity
PPLX_API_KEY=pplx-...
PPLX_MODEL=sonar
```

Health-Check 2.0

- `/api/monitor/check-keys` - Keys-Status ohne echte Calls
- `/api/monitor/health-check` - Mini-Pings mit Latenz-Monitoring
- Frontend zeigt Ampeln: 🟢 OK, ⚪ N/A, 🔴 Fehler

⚠️ Wichtige Hinweise

- **Niemals Keys in Code committen**
- **Niemals Keys in Logs ausgeben**
- **Niemals Keys in Tests verwenden** (nur Mocks)

- `.env.local` **hat immer Vorrang** vor `.env`
- **Health-Check zeigt nur Status**, keine echten Keys