OpenClaw 資安防護守則（必讀）

閱讀前必讀

- **這是什麼？**：OpenClaw 的資安與隱私防護守則
- **何時需要看？**：安裝前、開始串接 API、要備份或分享資料前
- **必要嗎？**：必要（避免金鑰外洩與資料風險）

目的：保護你的 API 金鑰、對話資料、Telegram Bot 與個人隱私。

---

1. 絕對不能外流的檔案

以下檔案一旦外流，任何人都能操控你的 AI：

- `~/.openclaw/openclaw.json`
- `~/.clawdbot/clawdbot.json`
- `~/.openclaw/keys/` 資料夾
- Telegram Bot Token

規則： – 不要上傳到 Google Drive / GitHub – 不要交給任何人 – 不要貼到群組或公開聊天

---

2. Telegram Bot 安全守則

- 不要外露 Bot Token
- BotFather 若懷疑外洩 → 立刻重置 Token
- 群組使用時建議：
  - 開啟群組權限審核
  - 避免給 bot 過高管理權限

---

3. 備份資料安全

備份資料可能包含： – 對話記錄 – API keys – 內部文件

規則： – 備份資料夾不要上傳到公開平台 – 如需傳輸，請使用加密壓縮檔（如：`zip -e`）

---

4. API Key 保護規則

- API Key 只放在本機環境變數
- 不要寫進任何 markdown / 教學文件
- 若有懷疑外洩，立刻旋轉（重建）API key

---

5. 公用電腦 / 遠端操作注意

- 不要在公共電腦登入 OpenClaw
- 遠端連線後記得登出 / 關閉 session
- 避免在共享螢幕時展示設定檔

---

6. 最佳安全建議（推薦）

- 定期更新 OpenClaw 版本
- 限制誰可以接觸你的電腦 / 控制台
- 有重要資料的檔案要分類管理

---

7. 如果懷疑被入侵

立即做這 3 件事： 1) 重置 Telegram Bot Token 2) 重設所有 API Key 3) 重新部署 OpenClaw

---

結論： 你可以把 OpenClaw 當作「AI 私人助理」。 但前提是你必須把金鑰與設定當成「你的銀行帳密」一樣保護。