附件二

AI 檢測申請單

填表日期：　　年　　月　　日

專案說明	承辦機關/單位/科室：		
	系統名稱：		
	使用目的：		
使用範圍	使用方式 (複選) *	□外部 AI　□租用 AI　□組織自建 AI □免費方案　□付費方案	
		請簡述：模型名稱、版本	
	主要佈署*	□公雲　□本地　□混合	
	環境與限制*	Rate Limit（頻率限制）	□是，頻率為_____ □否
		是否為正式環境	□是 □否
	使用類型*	生成式 AI	□AI 程式助理　□AI 對話助理 □AI 寫作助理　□AI 會議助理 □AI 媒體服務
		鑑別式 AI	□AI 分類　□AI 數據分析 □AI 辨識系統(影像/車牌/人臉)
		□其他：	
	運用方式*	□查詢資料　□資料分析　□程式開發　□教育訓練 □媒體生成　□文稿輸出　□其他：	
	使用者 共同責任*	身分管理：□組織帳號　□個人帳號　□無	
		設備管理：□公務手機/平板/電腦 □個人手機/平板/電腦　□無	
		存取管理：□多因子驗證　□密碼登入　□無	
		資料連接：□連接 Google/Microsoft OneDrive □本地文件上傳　□無 □其他：	
連線與測試憑證	Chatbot 存取網址	請填寫可供測試之 Chatbot 存取網址 範例：https://chat.example.com/llm	
	測試用 Token	(請填寫 Token 字串)	
		Token 有效期限：___年___月___日 (檢測完成後建議立即撤銷)	

<table>
<tr><td rowspan="2"></td><td rowspan="2">Token 權限說明</td><td colspan="2">(請簡述功能，如：僅對話/可呼叫 API)</td></tr>
<tr><td>是否為僅限測試用 Token</td><td>□是 □否</td></tr>
<tr><td rowspan="3">資料範圍</td><td colspan="2">輸入資料類型
(複選) *</td><td>□機密資料 □內部資料 □一般資料
□客戶資料 □個資(請勾選以下個資類別) □其他</td></tr>
<tr><td rowspan="2">※
個
資
類
別</td><td colspan="2">個人資料：
□姓名 □出生年月日 □國民身分證統一編號 □護照號碼
□特徵 □指紋 □婚姻 □家庭 □教育 □職業
□聯絡方式 □財務情況 □社會活動
□其他：得以直接或間接方式識別該個人之資料</td></tr>
<tr><td colspan="2">特種個人資料：
□醫療 □病歷 □基因 □性生活 □健康檢查 □犯罪前科</td></tr>
<tr><td rowspan="2">輸出檢查</td><td colspan="2">*是否有應受保護的系統提示詞(System Prompt)</td><td>□是 □否</td></tr>
<tr><td colspan="2">*模型是否可執行外部動作（如：寄信、交易、存取 DB、呼叫腳本、API）</td><td>□是 □否</td></tr>
<tr><td rowspan="6">其他</td><td colspan="2">*是否使用 RAG/向量資料庫？</td><td>□是 □否</td></tr>
<tr><td colspan="2">*是否可代表企業角色對客戶進行自由對話？（如：客服/諮詢 chatbot）</td><td>□是 □否</td></tr>
<tr><td colspan="2">*是否可提供 SBOM 以進行白箱式供應鏈安全檢視？</td><td>□是 □否</td></tr>
<tr><td colspan="2">*有無可能之敏感資料（如：PII、商業機密、醫療/財務）進/出模型</td><td>□有 □無</td></tr>
<tr><td colspan="2">*是否有流量限制或成本壓力？</td><td>□是 □否</td></tr>
<tr><td colspan="2" rowspan="2">*是否有備份還原機制
(避免模型汙染)</td><td>□是</td></tr>
<tr><td>□否（請簡要說明原因與風險控管方式）
_____</td></tr>
<tr><td>申請單位簽核</td><td colspan="2">承辦人：

日期：</td><td>機關首長或其授權人員：

日期：</td></tr>
<tr><td rowspan="2">實驗室審核</td><td colspan="2">單號：
單號 QRcode 黏貼區</td><td>審核意見：</td></tr>
<tr><td colspan="2">承辦人：

日期：</td><td>單位主管：

日期：</td></tr>
</table>