

附件 1-2（對受託機構／廠商及其負責人簽署）

《受託機構／廠商使用 AI 工具連帶保證書》

立保證書人受託機構／廠商（名稱：_____，統一編號／扣繳編號：_____；承接專案計畫名稱：_____），茲代表本機構／公司聲明並承諾，督導指派執行旨揭專案之所有團隊成員、計畫主持人、受僱人、派駐人員及顧問，均遵守環境部及所屬機關（構）（以下簡稱本部）所定「環境部及所屬機關（構）文件資料使用 AI 管理原則」（以下簡稱本原則）、契約、本保證書及相關法律義務。本機構／公司對專案執行期間因履約持有、知悉或接觸之本部文件資料（含本部執行各項業務所產生之文字、影像、聲音、資料庫、結構化及非結構化等資料），負監督管理及連帶保證責任，並承諾以下事項：

一、受託機構／廠商監督管理與資安控管條款：

- （一）本機構／公司承諾監督所有參與專案人員遵守本原則及本部資通安全、個人資料保護、保密與智慧財產權相關規範；並確保專案人員於接觸本部文件資料前，以書面切結適用本原則，且於接收第二級以上文件資料前，完成簽署本部所定保密切結書（含附件 1-1，如本部另有指定者從其指定），並造冊交由本部備查。本機構／公司及專案人員應依本部以書面或任何可儲存且可事後追溯之數位方式告知、標示、交付清冊或通知之分級使用本部文件資料；分級有疑義時，應即洽本部文件主責單位，未釐清前從嚴處理；文件資料內容異動或擬經不可逆去識別化處理後改變使用方式時，應洽本部重新評估分級及核可。
- （二）本機構／公司持本部文件資料使用 AI 工具，應依本原則及本部通知之工具、帳號辦理。第一級公開文件資料得使用商業生成式 AI 工具；第一級及第二級文件資料使用 AI 工具之輸出內容，均應經人工核實後始得正式運用。第二級內部文件資料限用環境部核定具備外部服務商資料不留存機制（服務提供商承諾不將使用者輸入資料及運算軌跡作為 AI 模型訓練或改善服務之用）之 AI 工具；外部人員持第三級以上文件資料使用之 AI 工具，由環境部環境資訊科技司提供或授權，其衍生經費由業務單位負擔；不得自行使用個人帳號、公司帳號、自費商業版或未經環境部核定、指定或授權之帳號或工具，將本部第二級以上文件資料輸入商業 AI 工具或外部雲端服務。

- (三)處理本部第三級（限閱文件資料）時，經業務單位主管核可後，限用環境部指定之封閉網路運算環境（如國家高速網路與計算中心算力環境）內之 AI 工具處理；經不可逆去識別化並經本部業務單位主管核可後，得比照第二級內部文件資料辦理。處理本部第四級（密等文件資料）時，嚴禁輸入任何商業 AI 工具或外部雲端服務；經本部業務單位主管核定後，限用環境部指定之封閉網路運算環境內之 AI 工具處理，並應依國家機密保護、資通安全及個人資料保護等相關規定從嚴辦理。第三級及第四級文件資料使用 AI 工具之輸出內容，應經人工核實並經本部業務單位主管核定後始得正式應用。
- (四)本機構／公司應建立內部 AI 使用防護機制，並依本原則留存使用紀錄；使用 AI 工具應留存使用紀錄至少六個月，使用紀錄至少保存半年，內容包括提示詞、附件、AI 工具輸出結果及操作帳號，並於本部稽核或查核時提供。未經本部授權，不得將本部文件資料、提示詞、附件或 AI 工具輸出內容私自複製、外傳，亦不得作為自身或第三人演算法模型之訓練資料。發現本部文件資料有誤傳、洩漏或 AI 不當使用情事，應即時向本部文件主責單位主管報告，並配合本部後續處置。專案結束或契約終止時，應督導全體專案人員立即停用因專案取得之本部 AI 工具使用權限；本部文件資料（含衍生資料與備份）除依法令或契約應保存者外，應返還、刪除或銷毀；依法令或契約保存者，仍應依原分級及保密義務控管，並不得私自留存其他副本。

二、法人責任與連帶保證條款：

- (一)本部得依契約、本原則及業務需要，定期或不定期派員就本專案涉及之本部文件資料、AI 工具使用紀錄、帳號權限及資安控管事項辦理檢查或稽核；本機構／公司及專案團隊應於必要範圍內配合提供資料及說明，不得無故拒絕、規避或妨礙；涉及非本專案資料、第三人營業秘密或個人資料者，應依法採取必要保護措施。
- (二)本機構／公司指派之專案團隊成員、受僱人、派駐人員、顧問或其他履約輔助人，如違反保密義務、本原則、契約或 AI 使用規範，致本部文件資料外洩、侵權、不當使用或本部受有損害者，本部得停止或通知受託契約方停止其接觸本部文件資料、系統或 AI 工具，依契約及本原則終止契約，並依民法、刑法、個人資料保護法、資通安全管理法、營業秘密法、著作權法及其他相關法令，請求本機構／公司負連帶損害賠償責任及追究法律責任；違約金（以契約已約定者為限）及鑑識、通知、補救、律師、訴訟等必要費用，依契約約定及相關法令辦理。
- (三)本機構／公司就前點連帶保證責任，於法律許可及契約約定範圍內，拋棄民法第 745 條所定先訴抗辯權；本部得逕向本機構／公司請求履行保證責任及損害賠償，本機構／公司不得僅以本部尚未先向違規個人求償或強制執行為由拒絕履行。

(四)本保證書對專案執行期間及因履約所接觸、持有或知悉之本部文件資料所生義務及責任，在法令或契約所定保存、保密、請求權時效及責任期間內，不因專案團隊成員離職、專案結束或契約終止而免除。

此致

環境部及所屬機關（構）

立保證書人受託機構／廠商名稱（蓋印大章）：_____

負責人／法定代理人姓名（代表簽章）：_____

統一編號／扣繳編號：_____

廠商聯絡電話：_____

廠商地址：_____

中華民國 _____ 年 _____ 月 _____ 日