**附件9 模型共享使用管理計劃**

子計畫名稱：3M Maker: 使用多模式、多任務、多事例學習開發可信賴多媒體處理技術(下稱本計畫)

計畫主持人：         廖弘源

資料集名稱：\_\_\_\_\_\_MS COCO\_\_\_\_\_\_ （**備註：各個資料集，須分別填寫不同份附件9**）

填表人：     陸玉霖

填表日期：  111 年  8 月 15 日

備註：下表一項資料集請填寫一份，表格不敷使用請自行增列。

**一、AI模型來源盤點程序**

計畫團隊應建立AI模型來源盤點程序，納入資料與模型治理作業規範中，主要盤點項目包括：授權型態、授權條款類型與版本、授權範圍與條件

|  |  |
| --- | --- |
| 事項內容 | 回應 |
| 關於「授權型態」，計畫團隊**所引用的程式庫**是採**傳統商業授權**或**自由/開源授權**？※備註：即使所引用的程式庫屬於自由/開源軟體(Free/Open Source Software)，也**不等同**於**可完全無償**且**無條件使用**。 | □ 傳統商業授權    ■ 自由 / 開源授權，授權條款 類型與版本為：**\*請繼續勾選** **\*若同個資料集採用不同套件，** **可複選** □ MIT ■ GPL（最嚴謹） □ LGPL □ APACHE □ Only new BSD license □ Simplified BSD license （最寬鬆） ■ 其他：\_\_YOLO\_\_\_\_\_\_ |
| **※前一題若選擇自由 / 開源授權者，才須回答此題**承上，關於「授權範圍與條件」，計畫團隊所引用的程式庫之授權條款對於利用該程式庫所「衍生」之作品，有無任何限制？就該「衍生」之作品，第三方使用者是否須透過**與原程式庫**（原作品）**同等條件**散布或再授權？※備註：所謂「衍生」 之作品即為「衍生著作」，係指就原著作**改作**之創作，以獨立的著作保護之，著作權法第6條訂有明文。 | □ 無任何限制（Simplified BSD license屬此）■ 有限制 **\*請繼續勾選** **\*以下限制由寬鬆到嚴格依序排列** **\*若同個資料集採用不同套件，** **應選取「最嚴格」的授權敘述**  □ 衍生之作品**可不共享**且可營 利，並且不可用原作者進行推 廣或推薦（Only new BSD  license屬此） □ 衍生之作品**可不共享**且可營 利，並且衍生作品**需要放置版** **權說明**（Apache、MIT屬此） □ 衍生之作品**必須共享**且**不可** **營利**，並且**不須**透過**同等條件** 散布或再授權（LGPL屬此） ■ 衍生之作品**必須共享**且**不可** **營利**，並且**須**透過**同等條件** 散布或再授權（GPL屬此） |
| 關於「授權範圍與條件」，計畫團隊所引用的程式庫，除了授權使用之外，是否能被複製、修改、合併、散布、再授權及 / 或販售予他人？ | ■ 是     □ 否 |
| 關於「授權範圍與條件」，計畫團隊所引用的程式庫之授權條款對於利用該程式庫所「衍生」之作品，有無任何限制？就該「衍生」之作品，第三方使用者是否須透過**與原程式庫**（原作品）**同等條件**散布或再授權？※備註：所謂「衍生」 之作品即為「衍生著作」，係指就原著作**改作**之創作，以獨立的著作保護之，著作權法第6條訂有明文。 | □ 無任何限制     □ 有限制，不過「衍生」之作品**不須**透過**同等條件**散布或再授權■ 有限制，而且「衍生」之作品**須**透過**同等條件**散布或再授權 |

**二、可信賴AI檢核程序**

|  |  |
| --- | --- |
| 事項內容 | 是否同意 |
| 計畫團隊應建立**可信賴AI檢核程序**，將可信賴AI檢核要求納入資料與模型治理作業規範中，並確保計畫團隊之落實。 | ■ 同意     □ 不同意 |
| 計畫團隊**應參考**科技部2019年提出的「人工智慧科研發展指引」(AI Technology R&D Guidelines) ，建立適切之**可信賴AI檢核表**，並依據檢核結果，思考或規劃當前或未來**可行的改善方法**。※備註：「人工智慧科研發展指引」(AI Technology R&D Guidelines)中由三大價值衍生構築出之 八大指引，包含「共榮共利、公平性與非歧視性、自主權與控制權、安全性、個人隱私與數據治理、透明性與可追溯性、可解釋性、問責與溝通」，詳參：<https://www.most.gov.tw/most/attachments/53491881-eb0d-443f-9169-1f434f7d33c7>  | ■ 同意     □ 不同意 |
| 承上，計畫團隊**應符合**科技部2019年提出的「人工智慧科研發展指引」(AI Technology R&D Guidelines)中之共榮共利指引。 | ■ 同意     □ 不同意 |
| 承上，計畫團隊**應符合**科技部2019年提出的「人工智慧科研發展指引」(AI Technology R&D Guidelines)中之公平性與非歧視性指引。 | ■ 同意     □ 不同意 |
| 承上，計畫團隊**應符合**科技部2019年提出的「人工智慧科研發展指引」(AI Technology R&D Guidelines)中之自主權與控制權指引。 | ■ 同意     □ 不同意 |
| 承上，計畫團隊**應符合**科技部2019年提出的「人工智慧科研發展指引」(AI Technology R&D Guidelines)中之安全性指引。 | ■ 同意     □ 不同意 |
| 承上，計畫團隊**應符合**科技部2019年提出的「人工智慧科研發展指引」(AI Technology R&D Guidelines)中之個人隱私與數據治理指引。 | ■ 同意     □ 不同意 |
| 承上，計畫團隊**應符合**科技部2019年提出的「人工智慧科研發展指引」(AI Technology R&D Guidelines)中之透明性與可追溯性指引。 | ■ 同意     □ 不同意 |
| 承上，計畫團隊**應符合**科技部2019年提出的「人工智慧科研發展指引」(AI Technology R&D Guidelines)中之可解釋性指引。 | ■ 同意     □ 不同意 |
| 承上，計畫團隊**應符合**科技部2019年提出的「人工智慧科研發展指引」(AI Technology R&D Guidelines)中之問責與溝通指引。 | ■ 同意     □ 不同意 |

三、AI模型提供使用（共享）之規劃

(一) AI 模型提供**使用條件**

|  |  |
| --- | --- |
| 事項內容 | 回應 |
| 是否需**對AI模型**的**使用對象**加以**限制**？※備註：只需要針對「填表當下目前已知資訊」去填寫 | □ 是，**AI模型**使用對象限於：      \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_■ 否 （包括**目前仍不清楚**是否需對AI模型的使用對 象加以限制） |
| 若預定上架的模型是**改作他人模型**，依據**原模型（改作前的模型）**的授權情況，預定上架的AI模型**需以何種方式再授權他人**使用？ | □ 傳統商業授權     ■ 自由/開源授權※自由/開源授權，包含：MIT授權條款(MIT License)、GNU通用公眾授權條款(GNU General Public License, GPL)等。 |
| 若預定上架的AI模型，是由模型提供者**完全原創**，依據**模型共享預期**的**目標**，預定上架的AI模型**需以何種方式再授權他人**使用？ | □ 傳統商業授權     ■ 自由/開源授權※自由/開源授權，包含：MIT授權條款(MIT License)、GNU通用公眾授權條款(GNU General Public License, GPL)等。 |

(二) AI 模型提供**使用方式**

|  |  |
| --- | --- |
| 事項內容 | 回應 |
| 依AI模型來源法律關係與可信賴AI檢核結果，**AI模型提供使用方式**為何？（例如：使用者可否取得程式原始碼等） | 使用方式：提供github連結及預訓練模型權重\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 如何**確保**AI模型取得是**安全**的？為避免AI模型發生**資安問題**，請說明所採用的手段。 | 手段 / 方案：提供github連結，可回報遇到的問題\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 承上，發生資安事故時，計畫團隊應如何處理？ | 處理方式：負責人因應所提出之問題進行應對\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

(三) AI模型**使用回饋**

|  |  |
| --- | --- |
| 事項內容 | 回應 |
| 計畫團隊**共享AI模型**所欲達成的願景或目標為何？ | 願景或目標：推動實時物件偵測之發展\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 承上，以此願景或目標為基礎，預期AI模型使用者要**如何提供回饋**？（可複選） | ■ AI模型使用成果預設授權予模型提 供者使用■ 使用者回饋有助於提升AI模型準確 度的訓練或測試資料□ 使用者回饋AI模型使用經驗□ 其他回饋方式：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

(四) AI 模型**使用情況追蹤**、**模型提供服務**之**改善**

|  |  |
| --- | --- |
| 事項內容 | 回應 |
| 計畫團隊採取**何種機制**以**瞭解**AI模型**使用的情況**？ | 所採用之機制：提供github連結\_\_\_\_\_\_\_\_\_\_\_ |
| AI模型**使用的情況**，是否符合**計劃以外使用者**的**需求或期待？** | ■ 是  □ 否□ 無從得知，因計畫外的使用者 沒有回覆 |
| AI模型使用過程中，**計劃以外的使用者**是否有發生問題或障礙？ | □ 是，發生的問題或障礙：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_■ 否□ 無從得知，因計畫外的使用者 沒有回覆 |
| 承上，計畫團隊在瞭解AI模型使用情況後，採取**何種機制**進行相應的改善或優化？ | ■ 技術團隊提供給**計畫外的使用者**  email或其他聯絡管道□ 其他機制：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| AI模型共享對**計劃以外的使用者**所產生之效益為何？※若無從得知，請據實填寫 | ■ 效益：\_有助於相關研究之進行 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□ 無從得知，因計畫外的使用者 沒有回覆 |

四、AI模型上架

是否有預計施行AI模型上架？ ■ 是，**請繼續填寫**以下表格   □ 否，**不需填寫**以下表格

|  |  |
| --- | --- |
| 事項內容 | 回應 |
| 計畫團隊將AI模型上架至共享平台**供他人使用前**，應先建立AI模型簡介或說明。 | ■ 同意     □ 不同意 |
| 計畫團隊若欲將AI模型放到「非自建」之共享平台供他人使用，AI模型**上架前**，計畫團隊應與「共享平台服務提供者」透過**委託書**、**契約**等文件，**預先議定**彼此的**權利義務**。**應注意**議定事項包括：(1) 預定上架及存放於平台的AI模型及期限（委託範圍與 期限）。(2) 委託範圍內AI模型品質之**維護方式**。(3) 平台對於AI模型之安全維護與**保密要求**。(4) 發生AI模型被竊取、竄改、毀損、滅失或洩漏等事故時， 平台之**通報義務**。(5) **要求平台**對其使用者（計劃以外的使用者）**規範**使用 AI模型的條件、形式與方法。(6) 違約責任。(7) 紛爭處理。 | ■ 同意     □ 不同意 |