**附件10 資安管理政策**

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

填表人：陸玉霖

填表日期： 112 年 5  月5  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、關於文件紀錄管控程序，是否同意以下事項**：

|  |  |
| --- | --- |
| 事項內容 | 是否同意 |
| 計畫團隊所建立的資安管理政策，應至少包括下列事項：  (1)**資訊資產管理**：建立資訊資產管理程序，識別計畫團隊之資訊  資產與定義適當之保護責任。  (2)**資安風險評鑑**：建立資安風險評鑑程序，識別、分析並評估計  畫團隊之資訊資產與使用情境可能產生的資安風險。  (3)**資安風險處理**：建立風險處理程序，針對資安風險評鑑結果，  選擇適切的風險處理方式，並採取必要的控制措施。  (4)**資安事故管理**：建立資安事故管理程序，確保計畫團隊對資安  事故作出迅速且有效的回應。 | ☑ 同意     □ 不同意 |

**二、關於資訊資產管理，是否同意以下事項**：

|  |  |
| --- | --- |
| 事項內容 | 是否同意 |
| 計畫團隊應識別計畫執行所需資訊及資訊處理設施之相關資產，進行**資訊資產的敏感性分級、分類或標示**，並將識別結果加以記錄 | ☑ 同意     □ 不同意 |
| 計畫團隊應給予資訊資產符合其敏感性等級的適切保護，應關注之事項**包括**但**不限於**：  (1)資訊資產的存取權限配置與控管、使用者身分認證，以及密碼  與金鑰管理。  (2)資訊儲存裝置之使用與控管，例如：隨身硬碟、行動硬碟等可  卸除式媒介，以及筆記型電腦、手機等行動裝置。  (3)資訊處理之實體環境安全與控管。  (4)惡意軟體之偵測與防範。  (5)資訊傳輸之安全與控管。 | ☑ 同意     □ 不同意 |

**三、關於資安風險評鑑，是否同意以下事項**：

|  |  |
| --- | --- |
| 事項內容 | 是否同意 |
| 計畫團隊**應識別**、**分析**、**評估**計畫執行過程中，**可能造成**資訊資產**失去機密性**、**完整性**及**可用性**之相關風險。 | ☑ 同意     □ 不同意 |
| 承上，常見的風險評鑑流程如下：  (1)**建立風險準則**：包括風險接受準則、履行資安風險評      鑑之準則。  (2)**風險識別**，而常見的**風險類別**包括：      A.人為：包含因人員有意或無意行為、人力資源管理不  當所產生的風險。  B.文件/資料：包含資料、文件的建立、維護、控管、  傳遞不當所產生的風險。  C.軟體：包含系統設計、維護、操作不當所產生的風險。  D.硬體：包含所有硬體設施之失效、毀損等可能風險。  E.通訊：包含資料、影像、聲音傳輸媒介失效所可能         產生的風險。  F.環境：包含天災、供水或用電等整體資訊環境可能         發生的風險。  (3)**風險分析**：依風險識別結果，分析風險發生的可能性      與可能導致的潛在後果（或嚴重程度），並決定風險      等級。  (4)**風險評估**：依風險準則，比較風險分析結果，訂定風      險處理優先順序。 | ☑ 同意  □ 不同意，本團隊**不同意之處**為：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  本團隊**採取之資安風險評鑑措施（必填）**：\_遵照流程建立風險準則、風險識別、風險分析及風險評估\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**四、關於資安風險處理，是否同意以下事項**：

|  |  |
| --- | --- |
| 事項內容 | 是否同意 |
| 計畫團隊應考量風險評鑑結果，**選擇適切的風險處理選項**，並對這些選項**設定必須的控制措施**或**訂定風險處理計畫**。 | ☑ 同意  □ 不同意，本團隊**不同意之處**為： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 承上，常見之風險處理選項包含四大類型：   1. 風險降低(risk reduction)：透過適當控制措施降低風險，若決定控制措施後，仍存在一些殘餘風險，應判斷是否可接受，如殘餘風險不可接受，應透過其他控制措施進一步解決。 2. 風險保留(risk retention)：若風險評估結果在風險準則可容忍範圍，則不需採行額外控制措施而能保留或接受風險。 3. 風險避免(risk avoidance)：當所識別的風險被認為太高時，應決定完全避免風險，退出已規劃或既有的資料處理活動，或變更活動運作的條件。 4. 風險轉移(risk transfer)：可決定與外界分擔某些風險，不過應注意風險轉移可能產生新的風險，或改變既有已識別的風險，且不應將重大風險轉嫁給資料當事人。 | ☑ 同意      □ 不同意，本團隊所採取之**其他風險處理選項**為： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**五、關於資安事故管理，是否同意以下事項**：

|  |  |
| --- | --- |
| 事項內容 | 是否同意 |
| 計畫團隊應建立有效的管理程序，確保**對資安事故作出迅速且有效的回應**。 | ☑ 同意     □ 不同意 |
| 承上，資安事故管理程序**應考量**：  (1) 資安事件**通報**：當發現異常情況或疑似資安事  件時，應依事件等級，依循適切的管道、時間，  對相關利害關係人進行通報，並研判該事件是  否歸類為資安事故。  (2) 資安事故**回應**：對資安事故進行危機應變處  理，並回覆相關利害關係人。  (3) **證據保存**：蒐集、取得與保存可作為證據的相  關資訊。  (4) **檢討與改善**：從分析及解決資安事故的經驗中  學習，進行事故成因檢討，改善資安管理作為，  並避免類似情況重複發生。 | ☑ 同意  □ 不同意，本團隊**不同意之處**為：  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    本團隊**所採取之資安事故管理程序**：  □ 依學校規定的資安事故管理程序  辦理  ☑ 其他：  \_依中研院規定的資安事故管理程序  辦理\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |