工業技術研究院
Industrial Technology Research Institute

AI 人工智慧應用安全與隱私技術

一、課程緣起：

隨著全球人工智慧（AI）迅速發展，眾多公司和投資資金紛紛投入人工智慧解決方案。隨著AI、物聯網與大數據持續地交互作用，我們越來越多個人資料被物聯網感測器蒐集，這一些大量資料被匯集成大數據，透過AI演算法不斷地分析與整合，即使原本是被匿名的資料，有可能被重新識別。AI應用越來越普遍，AI本身需要考量或是面對的安全與隱私攻擊，更是未來在開發AI應用所應該同步考量，因此本課程旨在巨量資料與AI應用下，講授資料在隱私方面的考量與相關技術，利用案例協助學員了解未來導入AI時需要注意的安全議題，並探討歐盟制定之Trustable AI帶來的影響。

二、課程目標：

本課程旨在巨量資料與AI應用下，講授資料在隱私方面的考量與相關技術，以及如何對應國內個資法、隱私安全標準以及GDPR等國際上的標準。

三、適合對象：

IT主管、工程師、AI創新應用規劃人員。

四、課程日期：

110年1/12，週二白天9:30 ~12:00,13:00~16:30 ，共1天、計6小時。

五、上課地點：

主辦單位：財團法人工業技術研究院 產業人才訓練一部(台北)
舉辦地點：工研院產業學院 產業人才訓練一部(台北)，實際地點依上課通知為準!!!!

六、報名方式：

報名方式：
(1)紙本報名：請以正楷填妥報名表傳真至02-2381-1000 黃小姐(02-2370-1111 分機304)
(2)線上報名：到工研院產業學院官網報名
課程洽詢：02-2370-1111 分機304/306 黃小姐

七、課程大綱：

單元	內容
資料隱私探討	● 國內外隱私法規與標準 ● 去識別化技術與應用範疇 ● 國內外資料隱私應用案例分享
AI應用的安全與隱私	● AI模型的安全與隱私

	● 對抗攻擊樣本 ● 深度偽冒 ● AI 安全與隱私的案例分享
AI 在隱私與安全上的解決方案	● 聯邦學習(Federated Learning)的應用案例 ● 聯邦學習之後的安全議題 ● Trustable AI 與 AI 國際標準趨勢 ● 導入 AI 應用的建議與討論

＊ 課程執行單位保留調整課程內容、日程與講師之權利

十、課程費用與繳費：

1. 本課程費用 NT$5,500 元(含稅），費用含課程、講義、餐點。
2. 開課前 10 天完成報名及並填寫繳費資料者，可享優惠價 NT$4,400 元（含稅)。
3. 招生及最低人數： 本課程預計招收人數為 30 人，至少需達 10 人才予開課。
4. 團報優惠：兩人團報可打 95 折、四人團報可打 9 折優惠。
5. 課程若未如期開班，費用將全額退還。
6. 繳費方式
   - ATM 轉帳（線上報名)：繳費方式選擇「ATM 轉帳」者，系統將給您一組轉帳帳號「銀行代號、轉帳帳號」，但此帳號只提供本課程轉帳使用，各別學員轉帳請使用不同轉帳帳號！！轉帳後，寫上您的「公司全銜、課程名稱、姓名、聯絡電話」與「收據」傳真至 02-2381-1000 黃小姐 收。
   - 信用卡（線上報名)：繳費方式選「信用卡」，直到顯示「您已完成報名手續」為止，才確實完成繳費。
   - 銀行匯款(公司逕行電匯付款)：土地銀行　工研院分行，帳號 156-005-00002-5（土銀代碼：005)。戶名「財團法人工業技術研究院」，請填具「報名表」與「收據」回傳真至 02-2381-1000 黃小姐 收。
   - 即期支票或郵政匯票：抬頭「財團法人工業技術研究院」，郵寄至： 100 台北市中正區館前路 65 號 7 樓 704 室 黃小姐收。
   - 計畫代號扣款(工研院同仁）:請從產業學院學習網直接登入工研人報名；俾利計畫代號扣款。

十一、報名確認與取消：

1. 已完成報名與繳費之學員，課程主辦單位將於開課三天前以 E-mail 方式寄發上課通知函；若課程因故取消或延期，亦將以 E-mail 方式通知，如未收到任何通知，敬請來電確認。
2. 已完成繳費之學員如欲取消報名，請於實際上課日前以書面通知業務承辦人，主辦單位將退還 80% 課程費用。
3. 學員於培訓期間如因個人因素無法繼續參與課程，將依課程退費規定辦理之：上課未逾總時數三分之一，欲辦理退費，退還所有上課費用之二分之一，上課逾總時數三分之一，則不退費。
4. 本單位保留是否接受報名之權利。
5. 如遇不可抗拒之因素，課程主辦單位保留修訂課程日期及取消課程的權利。

※注意事項※ 為確保您的上課權益，報名後若未收到任何回覆，請來電洽詢方完成報名

【傳真報名專線：02-2381-1000 黃小姐收】

AI 人工智慧應用安全與隱私技術

公司全銜					統一編號	
發票地址					發票方式	□二聯式(含個人) □三聯式

姓名	部門	職稱	電話	手機	E-mail (請以正楷書寫)	膳食
						□素
						□素
						□素

聯絡人	姓名	部門	職稱	電話	傳真	E-mail (請以正楷書寫)

繳費方式：

□ ATM 轉帳（線上報名）：繳費方式選擇「ATM 轉帳」者，系統將給您一組轉帳帳號「銀行代號、轉帳帳號」，但此帳號只提供本課程轉帳使用，各別學員轉帳請使用不同轉帳帳號！！轉帳後，寫上您的「公司全銜、課程名稱、姓名、聯絡電話」與「收據」傳真至 02-2381-1000 黃小姐 收。

□ 信用卡（線上報名）：繳費方式選「信用卡」，直到顯示「您已完成報名手續」為止，才確實完成繳費。

□ 銀行匯款(公司逕行電匯付款)：土地銀行　工研院分行，帳號 156-005-00002-5（土銀代碼：005）。戶名「財團法人工業技術研究院」，請填具「報名表」與「收據」回傳真至 02-2381-1000 黃小姐 收。

□ 即期支票或郵政匯票：抬頭「財團法人工業技術研究院」，郵寄至： 100 台北市中正區館前路 65 號 7 樓 704 室 黃小姐收。

□ 計畫代號扣款(工研院同仁)：請從產業學院學習網直接登入工研人報名；俾利計畫代號扣款。

總計 課程費用
$_____

歡迎您來電索取課程簡章～服務熱線 02-2370-1111～工研院產業學院 產業人才訓練一部(台北) 歡迎您的蒞臨～

*本課程歡迎企業包班~請來電洽詢 課程承辦人 黃小姐 02-23701111#306