麥寮鄉公所政風室 115 年 4 月機關安全維護宣

1.AI 軟體與服務可能產生之風險疑慮

近年來 AI 軟體與服務快速發展，影響遍及全球產官學研各界。自 ChatGPT 於 2022 年底發布後，更掀起全球熱潮，且被視為人工智慧之一項重大突破。運用生成式 AI 軟體與服務協助執行業務或提供服務，有助於提升工作效率與創意發想。

AI 軟體與服務常透過蒐集使用者輸入內容或擷取網頁文字做為訓練資料，以逐步改善模型並產出更正確之結果，故可能涉及隱私洩露之風險。另外，AI 軟體與服務透過大量蒐集與訓練所產出之結果，可能涉及侵害智慧財產權、人權或商業機密之風險，且受限於訓練資料之品質與數量，可能會生成真偽難辨或創造不存在之資訊，建議針對生成結果需進行評估後再行運用。

使用 AI 軟體與服務時，應避免暴露個人資料與機敏資訊，同時注意內部保密義務與智慧財產權相關規定，秉持負責任及可信賴之態度，掌握自主權與控制權，並堅守安全性、隱私性與資料治理、問責等原則，不得恣意揭露未經公開之公務資訊、不得分享個人隱私資訊及不可完全信任生成資訊。

此外，有鑑於過往曾發生軟體與 APP 被發現重大資安疑慮情事，近期 AI 軟體與服務如雨後春筍般誕生之際，亦難免出現相似資安疑慮，因此選用 AI 軟體與服務時，需留意提供該軟體與服務之公司背景，不應盲目信任使用。

隨著針對不同使用情境不斷推陳出新之 AI 軟體與服務，建議企業與民眾使用前審慎評估軟體是否安全，輸入之資料是否敏感，並了解軟體開發商之隱私權政策及如何處理資安漏洞等問題，以免發生違法、洩漏敏感資訊、侵害智慧財產權及財物損失之憾事。若欲於工作中採用 AI 軟體與服務，可參考「行政院及所屬機關（構）使用生成式 AI 參考指引」，以降低可能帶來之危害與風險。

2.數位時代的保密防諜

「保密防諜、人人有責」這句口號，對六、七年級生來說，相當的陌生，但是對四、五年級的讀者而言，卻是非常的熟悉，以前不但在社區的牆壁上會看到它，在學校、部隊…等各種重要場合都可以看到這個標語。民國五０、六０年代，兩岸關係緊張，可謂是漢賊不兩立，雙方都有間諜在探視彼此的活動，到了民國九０年代，兩岸交流絡繹不絕，敵我意識漸漸模糊，保密防諜的口號亦漸漸式微。

想必大家都看過 007 情報員或長江一號之類的諜報電影，其中的間諜可能要透過特殊設計的照相機，把所獲得的資料拍下，再放到牙齒或身體的某處做為掩飾，再經過層層的轉送，才能傳回總部。

隨著資訊科技的進步，現在的 007 情報員不需要再用特殊設計的相機，時下的數位相機愈來愈輕薄短小，手機也多附有照相功能，要拍下重要資料是輕而易舉的，而且所有的資訊都資訊化、數位化，透過無線傳輸的技術，更是可以神不知鬼不覺的偷走機密資料，幾乎人人都可以當情報員。

在數位時代裏，不止是政府機關或是軍事部隊需要保密防諜，企業對機密資料的保護更是不遺於力，數位資料的特色是很容易被偷，而且被偷了也不容易被查覺，本文將介紹在數位時代中，企業機密資料的外洩管道，及各個企業如何防止公司的機密資料外洩。

根據微軟內部調查顯示，去年臺灣有近 1000 萬人次申請下載使用 MSN 軟體或申請帳號，35 歲以下的民眾，八成有使用 MSN 的經驗。研究機構 Yankee Group 針對全球即時通訊工具的市場研究報告指出，今（94）年底全球使用即時通訊（包括 MSN、Yahoo Messenger…等）的人數將會超過 3 億人，不少的企業都肯定即時通訊軟體的工作效率，如國內的 3c 大廠 NOVA，很早即利用即時通訊軟體來進行內部溝通。

資訊科技愈來愈發達，照理說使用這類軟體的公司應該也愈來愈多，但是，報載自今(94)年五月四日起，摩根富林明資產管理集團(JPMorgan Fleming Asset Management）全球的 16.4 萬名員工上班全面禁止使用 MSN，這又是甚麼原因？難道是怕員工上班時在網路上聊天？隨著 MSN、Yahoo Messenger…等通訊軟體的普及度越來越高，只要輕輕的敲擊鍵盤，公司機密即無所遁形，大部分企業對於其威都非常恐懼，特別是科技園區、金融單位不少企業明文禁用 MSN、Yahoo Messenger…等通訊軟體，主要都是怕機密的技術資料或者是客戶資料，透過 MSN、Yahoo Messenger…等通訊軟體傳給競爭對手。

除了 MSN、Yahoo Messenger…等即時通訊軟體外，企業洩漏機密的另一管道是電子郵件（E-MAIL），很多的企業為了防止這個洩密管道，都

對電子郵件的資訊量及內容做管制，並且在郵件伺服器（Mail Server）上記錄員工傳送的資料，以便後續追查，雖然，此舉曾造成是否侵犯員工通訊隱私權的爭議，但是，為了維護公司機密的安全，各公司仍然採用此方式管制電子郵件。

萬用串列匯流排（Universal Serial Bus，USB）已成為資訊媒體新興的標準介面，只要擁有該介面的電腦週邊設備，都可以透過它來上傳或下載資料，加上行動碟與可攜式硬碟的容量都愈來愈大，一些大的檔案原來透過3.5吋的磁碟片不易下載、攜帶，此時都可以經由USB介面很容易的被下載、攜帶了。很多的公司為了防止員工藉由USB介面下載資料，會在員工的個人電腦上安裝偵測程式，一旦員工藉由USB介面傳輸資料，即會啟動網管安全機制，以維公司資訊的安全。

當然，為了釜底抽薪，有的公司甚至於把電腦上所有可傳輸資料的週邊設備全部拿掉，如燒錄器、軟碟機、USB介面…等，以免員工有機會下載資料，俾能有效管理資訊的安全。

除了以上的防制作為外，很多的高科技公司為了讓公司內部的資訊不易被外界的駭客破壞或竊取，將公司內部的網路與外部網路進行實體隔離，讓外部的人無法接觸公司的資料，但是，這樣有好也有壞，公司外部的人雖然無法接觸公司的資訊，相對的，公司的員工在外面也不能獲取公司的即時資訊。

現在的消費性電子產品的功能愈來愈多，也做的愈來愈精巧，如具有照相功能的手機、個人數位助理(Personal Digital Assistant，PDA)…等，都具有儲存影像、資料及錄音等功能，均可能成為洩密的管道，很多科技公司不但管制員工使用，也要求訪客不能帶入公司，必須放在大門由保全人員或警衛先行代為保管，俟離開時再取回。

以上所談的都是企業對內部員工的管制作為及對訪客的限制，其目的不外乎就是維護公司的資訊安全，數位時代中資訊的價值愈來愈高，相對的，機密資料外洩後所需承擔的代價也是不可承受的高，我們在想受豐富資訊的同時，不能不想到保密的重要性。