114年10月公務機密宣導-

紙本個資文件防護

因應紙本個資文件防護需求，機關應從管理面出發，並搭配技術面輔助管控，像是在列印設備上早已提供諸多功能協助管控，包括身分驗證、權限控管、機密列印與紀錄備存等功能，妥善利用這些功能，便能強化列印設備與紙本文件的個資防護，減少紙本文件帶來的個資風險。

★紙本文件輸出缺乏有效管控

舉例來說，列印時，一旦有個資內容的文件印出後被他人誤取，或無人領取，就是紙本個資在列印時造成的風險缺口。傳真也是紙本個資防護不能忽略的管道，像是傳真文件印出被人拿取，下班時間後輸出的傳真文件沒人控管，也會造成同樣的問題。

從個資文件的產生、傳遞、利用，直到最後的銷毀與保存，都應制定好各人員的授權與責任，同時建置機密文件的分類、分級制度，並檢視現有作業流程。而員工的個資防護教育訓練也是持續不斷要做的事，讓員工不論是在業務流程中，或是工作習慣上，都應該有良好的個資防護觀念。

★列印工作若委外，交付企業仍有個資責任

除了自己內部列印的管控，有些機關也會將文件列印工作委外處理。但委外並不代表機關不用負責，依據個資法第 4 條規定，「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」因此，機關在交付個資文件委外作業時，需要謹慎評估，並針對有關個人資料處理的業務，建立評估的標準，以便篩選出適合的配合廠商。

★紙本資料輸出後，形成管理大漏洞

過去許多列印、傳真、掃描的使用習慣，其實都是紙本個資文件管控的大漏洞，管理者應立即檢視這些問題所帶來的個資風險。

漏洞 1 列印文件擱置在設備上，遭誤取或窺視
漏洞 2 個資文件傳真進來後，在傳真設備上無人領取
漏洞 3 傳真個資文件時，不小心傳送到錯誤對象
漏洞 4 掃描歸檔結果輕易被他人存取

★列印前的控管做法：個資文件印出前，應先做好列印行為權限管控不論是從列印設備開始管控，或是針對檔案限制使用者的列印權限，均可減少紙本機密、個資文件的管控。

【資料來源：臺中市政府水利局政風室】

114年10月機關安全維護宣導-

資訊安全的四項提「防」

隨著電腦應用的普及和網際網路的急遽發展，不僅改變了人類的生活模式，也帶來令人憂慮的資訊安全問題。因此，建立完善的資訊安全防護措施已是當務之急，唯有在安全無慮的前提下享用網路資訊帶來的便利，才是面對科技發展的正確態度。

資訊安全的種類可分為三個面向：一、硬體的安全，包含對於硬體環境的掌握以及設備管理;二、軟體的安全，包含資料軟體安全和通訊管道的安全性;三、個資的安全，包含個人資料保密，隱私性等。

如何做到上述資訊安全的保護措施呢？首先我們要了解影響資訊安全的因素，包括：未經授權侵入使用者帳戶，進行竊取或是更動系統設定;資料在傳輸過程中被擷取，或被變更內容;透過感染電腦病毒與傳播惡意程式。諸如此類的資訊安全問題層出不窮，且手法日新月異，然而注意下面幾點防護措施，可在面對大部分的狀況時，具備基礎的防護手段。

一、防毒：當一隻病毒被製造出來之後，開始於電腦與網路設備中擴散，透過網絡無遠弗屆的傳遞，變成所有電腦使用者的夢魘，隨之而來的系統崩潰甚至硬體損壞，將損毀寶貴的資料。使用者防治的積極手段就是安裝來源合法的防毒軟體，並且定時更新病毒碼，以保持作業系統處於健全的防護程度。

二、防駭：隨著社群網絡和各式資訊系統的應用，駭客由開始時半開玩笑地更動系統設定，演變到後來的蓄意破壞、資料竊取，也因此發展出了各式的系統安全通行證，包含使用者密碼、身分驗證、通訊鎖、晶片卡等設置，普遍使用於各層面。除了定期變更驗證方式以及使用多種防護作為外，也需隨時保持資安的

警覺性。

三、防治天災：這是容易忽略的一個項目，電腦硬體從來就屬於耗損型的設備，隨著時間、溫度、濕度、跳電等，甚至震動都可能導致硬體的受損;因此使用者應該以嚴肅的態度準備更完整的防治計畫，例如定期更新易耗損的硬體設備，備份重要資料，以及安裝備用，預防斷電造成的資料損失等。

四、資料防竊：隨著智慧型手機的流行，現在低頭族已成為一種社會現象。而資訊的氾濫成為眾多使用者頭痛的問題，許多不同的應用程式都會記錄使用者的個人資訊，但設計這些應用程式的公司是否確實做好保護我們的個人資料？值得存疑！許多應用程式的分享與協同編輯功能權限設置不明，更是成為資料安全上的一大隱憂。因此，我們對於自身的資料處理應該抱著更謹慎的態度，切勿在網路上分享或是儲放機密資料。我們若能認真地思考資安問題，完善規劃這些資訊系統與網路設備，定期保養與維護個人資安，便可長保資料的可用性及可靠性了。

【資料來源：法務部調查局】