避免個資外洩的應注意事項

一、申辦政府機關、金融機構等各種業務，需要提供個人資料以及身分證等證件，務必在繳交證件影本上註明「僅供申辦○○業務使用」，以免不慎資料外流被不肖分子移做他用，使自己成為人頭帳戶。

二、每個月的帳單明細、ATM 交易收據、申辦各項業務作廢的申請書或其他任何記有個人資料的便條紙，只要是有關個人資料，都應小心處理。建議可使用碎紙機處理，若無碎紙機時，也應將重要資訊部分重複撕毀，切勿隨手丟棄。

三、隨著資訊的發展，透過網路行為所造成的資料外洩有逐漸增加的趨勢。除了來路不明的網站別亂點擊，以免被植入惡意程式之外，所使用的瀏覽器也必須符合 SSL 或 SET 的安全標準，這樣才能確保在網路上進行交易時的資料是經過加密處理的；此外，P2P 等分享軟體所造成的「個人資料分享」也是時有耳聞，在使用上也必須特別小心。

四、勿用過於簡單的帳號密碼，無論是提款卡的密碼、網路上各項服務的帳號密碼，請勿用生日、電話、身分證字號等容易識別個人身分的字串，以免當卡片遺失或是帳號被盜取時，密碼被輕易地猜測出來。

五、近年來因送修含有儲存裝置的3C產品所造成的個人隱私外洩事件層出不窮，教人不得不警惕。若因3C產品故障需送修時，應確保個人相關資料已妥善處理，以避免資料外洩。

六、申辦加入會員，在提供個人資訊前，應詳閱說明及相關保密政策，是否有選擇不將資料提供給其他廠商的欄位，以免個人資料不當流出。

七、參加摸彩活動、路上隨機的問卷調查，這些看似不經意的資料填寫，常常讓我們在不自覺中將個人資料流出，所以在填寫時應盡量避免填寫重要的個人資訊，留下的資料越少越好。

總之，個資外洩防不勝防，除了平時應養成良好的習慣外，切勿隨意提供個人資料並避免不當的網路行為，而在提供個人資料以申辦各項業務時亦須十分小心；當遇到疑似詐騙電話時，更應冷靜以對，小心求證，切勿驚慌，以免造成更大的損失。

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；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，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：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：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，以及安裝備用電源，預防斷電造成的資料損失等。

四、資料防竊：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。

公務機密維護宣導-公務資料外洩案例

[案情摘要]

某政府機關主管○○○習慣將經手公文之電子檔拷貝留存備用，並經常以隨身碟再將其拷貝至家中電腦硬碟儲存運用，其家用電腦遭駭客植入後門程式而不自知，以致長期大量經手之機密文書陸續外洩。

[處理經過]

本案○○○私下將機密文書攜離辦公處所，致長期大量經手之機密文書陸續外洩，經調查單位查獲且依法偵辦，影響機關形象。

[檢討分析]

由本案例我們可知公務人員處理公文案件若疏於注意，違反保密規定，往往造機關或個人損害，依電腦處理個人資料保護法第 17 條規定：「公務機關保有個人資料檔案者，應指定專人依相關法令辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」，另外依刑法第 132 條：「公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處 3 年以下有期徒刑、拘役或 3 百元以下罰金。因過失犯前項之罪者，處 1 年以下有期徒刑、拘役或 3 百元以下罰金。非公務員因職務或業務知悉或持有第 1 項之文書、

圖畫、消息或物品，而洩漏或交付之者，處1年以下有期徒刑、拘役或3百元以下罰金。」因此，雖然政府機關對資訊安全重視。然而，公務員將公事攜回家中處理之情形仍十分常見，但家中個人電腦防護力較低，容易遭駭客入侵致公務資料外洩，不但涉及行政責任，更須負刑事責任，因此為保護公務資料之安全，平時應該更加謹慎注意。

保防宣導-----網路危機防範

社會快速變遷，網際網路已為人類帶來了不少便利。對於E世代新新人類而言，網路是學習新知最重要的方式之一。從網路上可以獲得資訊並累積資訊，但是藉由網路散布資訊所帶來的潛在危害，及利用網路來從事犯罪行為，更將成為社會的一大隱憂。青少年常因為對法律概念認識不清，身陷危險而不自知。為此，我們提供網路危機防範守則及兒童及少年性交易防制條例等相關法令，希望能協助青少年認識網路危機、遠離危險。

・ ・網路交友新鮮刺激，但危機重重。勿迷惑於華麗的虛擬情境，而使自己落入陷阱、無法自拔。

・ ・網友相見不要貿然赴約。即使赴約，也應特別提高警覺。最好由親友陪同前往，並了解約會行程，選擇安全約會地點，並堅持行動自主之立場。

・ ・對於個人資料的登錄要小心謹慎。在網路上儘量避免留下真實姓名、電話、住址、信用卡帳號等基本資料。

・ ・慎選聊天室與網站。

・ ・遵守網路基本禮節。在網路世界中仍要以誠待人，不要做出任何傷害他人的事情。

・ ・網路交友「二要、三不」：

二要：

- 家長「要關心、放心」，對於子女使用網路的情形多關心，對於子女正當使用網路能多放心。
- 親子之間「要約法三章」，約定如何正當使用網路。

三不：

- 「不沉迷」網路而影響功課或身體健康。
- 「不暴露」自己相貌及個人隱私資料。
- 「不私下交往」，保護自己與家人安全。

冒牌銀行利用網路詐欺、假冒信用卡公司利用網路刊登檢測偽卡程式，常在取得帳號密碼及卡號後進行盜領及盜刷行為，運用網路購物及利用網路銀行理財者，應慎防詐騙，以免得不償失。

現代政府機關機密維護工作從個人做起

現代機關機密維護工作並不是要把身旁每個人都當作假想敵，處處提防著別人，應該從強化教育自我保密觀念、隨時養成機密維護習慣、確實遵守資訊保密規定，從以下這幾個重點著手：

一、強化教育自我保密觀念：平時加強同仁機密維護教育宣導，強調機密維護工作對關安全的重要性，機關安全需要同仁共同經營，以教育的方式，使同仁經由潛移默化的方式，培養「機密維護工作

就在你我」的觀念。

二、隨時養成保密工作習慣：貫徹機密維護工作的最佳方法，是將機密維護觀念落實在生活，進而成為「習慣」。養成機密維護工作習慣可以從許多方面著手，例如離開機關不談公事、離開辦公桌時公文應放置於公文櫃內並加鎖、休假前辦公室應確實上鎖等。

三、確實遵守資訊保密規定：根據統計，資訊洩密違規事件肇生原因有20%是因為軟、硬體遭外力突破等；而約80%大多數的原因是由人為因為所造成，其中大部分又是由於違反資訊保密規定所造成的洩密違規事件。

因此杜絕資訊洩密違規事件最好的方法便是從每一位資訊系統操作者著手，例如平時養成使用資訊設備、電腦的良好習慣，個人電腦帳號密碼依規定設定，帳號密碼確實保密並定期更換，資料檔案依規定加密壓縮後才可使用電子郵件或伺服器傳送，並嚴禁使用隨身碟、燒錄器、讀卡機等個人資訊存取裝置。倘若每一位資訊系統操作者能從本身做好資訊保密工作，依規定操作資訊設備，便能減少資訊洩密違規事件發生的機率，確保資訊保密安全。「機密維護工作從個人做起」並不只是個口號，而是需要每一份子共同努力及遵守的目標。平時養成保密習慣、確立自我機密維護觀念、機關安全必能確實獲得保障。

高雄市梓官區公所政風室關心您