機密維護常識彙編（102 年 1 月份）

＊淺談機敏會議資料保密作為

保密作為及可行方式如下：

一、研訂機敏會議保密措資料施為落實機敏會議資料保密機制並明示保密責任，政府機關應審慎評估自身業務特性並研訂保密措施，內容建議如下：

（一）機敏會議資料應使用隔離電腦處理，不得使用於連結網際網路之電腦設備。

（二）機敏會議資料相關檔案及紙本均應加註「機敏資料」之浮水印文字。

（三）機敏會議資料首頁註記「本資料因具機敏性質，相關人員應行保密」等文字，並應分別編號。

（四）會議使用不可攜回之機敏資料，均應於會議後按編號收回，若因公務需要留用，應經主席核准並簽收。

（五）召開機敏會議時，於會議開始前，主辦單位應提示與會人員知悉，並於簽到表上註記「本會議因具機敏性質，與會人員應行保密」等文字。

（六）禁止透過網際網路（如電子郵件）傳送機敏會議資料；惟若確因公務需要透過網際網路傳送者，應刪除涉密內容，該部分資料則另採書面發送並經簽收程序。

（七）退休離職或職務異動時，在職期間所經手或保存之機敏資料，應列入移交或依規定銷毀。

（八）機敏會議應以秘密方式舉行，並選擇單純或有隔音設備之場所以防止竊聽，同時禁止非相關人員隨意進出。

二、加強保密宣導以及教育訓練

由於機敏會議資料外洩多屬人為因素，其中又以機關同仁故意或疏失者居多，因此欲降低資料外洩的機率，最主要應從培養同仁保密觀念著手。各機關應將現行法令規定、內部保密措施、洩密案例以及可能導致洩密管道等，透過教育訓練或機關內部網路等方式加強宣導，務使每位同仁均能了解相關保密規定、法律責任及具體作為，以養成落實機敏會議資料保密之習慣。

三、落實資訊安全稽核

為機先發掘資安漏洞，同時檢視機關同仁實際執行保密情形，政府機關應定期或不定期（如當發生重大洩密案件時）執行資安稽核檢查，藉此改善缺失並提高防火牆功能以防駭客入侵。

四、將機敏會議資料列入保密檢查之重點項目

因機敏會議資料多屬公文之附件，故亦為機密文書之範圍。準此，其是否以機密文書之方式辦理收發、傳遞、歸檔、清查、機密等級變更（或註銷）及銷毀等程序，應一併列入公務機密維護檢查項目。除藉此檢討相關保密措施是否確實及督促同仁提高警覺外，並可發掘洩密案件線索，實具多種意義。

五、強化主管考核監督

單位主管對於該管業務及屬員狀況最為了解，故若能落實業務督導及人員考核，自可發揮防患於未然之效果。當單位主管處理屬員所簽辦之機敏會議資料時，除應善盡督導之責外，若屬員有工作不力、交往複雜、財務狀況不良、經濟來源可疑，或曾遭檢舉操守風評不佳時，則應加強輔導考核作為，並適採必要之防處作為，以防範洩密情事發生。此外，對於執行良好者從優獎勵，對於執行不力者則依規定懲處，藉以促使機關同仁重視保密工作並具體執行。

（本文摘錄自清流雜誌-李志強）

＊建構全方位網路安全防護網

這是一則刊登在各大報刊的廣告，內容明確揭示：企業如因內部機密資料外洩，將面臨客戶流失和巨大的財務損失，亦嚴重危害企業主營運績效。案內廣告提醒企業主，在一片不景氣中，擬將採取緊縮編制及裁員策略之同時，別忘了做好防範企業機密資料外洩的準備。

這則廣告亦同時提醒我們，隨著資訊科技一日千里，網路及電腦已成為資訊取得的重要來源，復以電腦輸出入裝置及隨身儲存載體的發達，若未能貫徹各項保密規定並做好防範措施，輕則個人資料外洩，重則影響組織運作及國家安全，實應予以正視。

刑事警察局於 97 年 3 月間破獲一起某企業員工離職後自行成立性質雷同之公司，

並藉由盜用舊公司帳號、密碼，入侵該公司資料庫，竊取價值 500 萬元國外競標訂單；此外，某購物台亦發生離職經理將客戶資料存入個人硬碟中，並盜賣 14 萬筆個資，獲取不法利益。近期，軍中也發生某退役軍官涉嫌於服役期間蒐集包含漢光演習、作戰計畫、通訊密碼，及人員、武器編裝等 9 萬件軍事機密級電子檔案資料，交付中共統戰部門在台人員，以索取巨額報酬的案例。

最近加拿大網路研究機構「資訊站監督人」(IWM) 於調查一宗網路駭客案件時，意外發現全世界 103 個國家的政府與民間電腦檔案，包括台灣駐外機構及達賴喇嘛等西藏流亡人士電腦裏的機密檔案，均曾遭到來自於中國大陸所謂「鬼網」的電子間諜所滲透攻擊。

從以上案例顯示，現今資訊科技不斷更新與網路蓬勃發展，雖帶給民眾生活諸多便利，但也衍生許多新的社會與犯罪問題，其中，最明顯的現象，就是資訊安全對於企業或國家所產生的衝擊與挑戰。

此外，根據統計，影響「資訊安全」威脅最大的是來自於人為的蓄意侵害，亦是資訊安全工作上最難預防的威脅因素。因此，資訊安全防護工作之良窳，攸關著網路世界是否能依照公平原則進行各項作業。

21 世紀是資訊科技發達的時代，其快速而有效率的特性，使得不論是在交通、金融、電力，乃至於國家行政系統運作上，都非常倚賴資訊系統做為各項作業及管理的工具。但是，「水能載舟，亦能覆舟」，雖然資訊科技建構了便利的使用環境及大幅提升行政運作的效率，卻也因為資訊系統本身的弱點，給予有心人士從事非法活動的空間；例如透過隱藏的病毒發動網路攻擊，讓電腦使用者難以事先察覺及預防，使資訊系統被破壞或遭受攻擊，造成重大損失。因此，面對資訊發展所形成危機四伏的資安威脅，世界各國紛紛採取各種綿密的防範措施，以杜絕重要資訊的外洩。例如：美國投入約 40,000 人力成立網路戰司令部，參與資訊攻防的相關工作；日本則由陸海空自衛隊電腦專家約 5,000 人組成網路戰部隊;巴基斯坦也組織了網路戰部隊,還曾在 2003 年與印度駭客展開網路大戰。我國則由行政院資安小組整合產、官、學界專業人士，建構全方位的資訊安全網，負責網路安全與防護的工作。

面對無孔不入的駭客，我們應如何強化資安防護，以確保機密資訊的安全呢？基本上，身處資訊時代，人人均應建立網路安全概念，並養成資訊防護的良好習慣，例如不將公務資料攜回家中處理、不隨意開啟來路不明電子郵件、隨身碟使用完畢後即予格式化、不隨意瀏覽不明網站、不執行郵件內夾帶的檔案或連結、避免下載免費軟體或圖檔、不隨意點選網頁內的連結網址或彈出式廣告或不明內容視窗、避免使用點對點軟體分享檔案、不使用駭客工具，及關掉不必要的網路服務等，只要多用一點心、時時自我提醒，就能有效遏制駭客從事的情蒐、竊密行為。

資訊安全工作是一項防患於未然的風險管理過程，只要人人建立「資通安全，人人有責」的觀念，且不斷提升資訊防護的技能，就能夠降低資安威脅，確保機密資料不外洩。

「患常起於所忽，禍多伏於忽微」，由於網路使用的普及性，導致駭客無所不在。而網路所掀起的「看不見敵人的戰爭」，面對這場「無煙硝戰爭」的威脅，我們應從資安教育做起，強化人人資安防護的概念、縮小保密習性及資安素養的差距，並建構縝密的資安屏障，方能有效因應資訊作戰的嚴格考驗，從而維護國家整體之安全。（以上資料摘錄自法務部調查局網站）

＊公務機密維護宣導

話說我國歷史上春秋戰國時代，齊桓公與管仲秘密決定代莒，惟尚未行動消息卻已傳遍全國，桓公質疑令查，結果發現係役人東郭郵所洩漏，而役人回答相公伐莒係其所猜測，而桓公再問役人，所據為何？役人回答，主公與管仲交談，口開而不闔，應是說莒國，舉手他指之方向亦當莒國，而當此時小國之中只有莒國尚未臣服；桓公聞言驚覺以一些細微之徵候即能判明伐國大事，自此管仲處理日常事務則更謹慎，並道出幾而不密殆、無翼而飛者聲也、凡道必周必密等名言，乃得襄助桓公完成霸業。

另說五代中吳國徐知誥與齊邱議事，總是選擇水心涼亭低聲商談，冬天兩人在大廳中問圍爐對坐，把周圍的屏風一律撤除，使旁人無法偷窺，他倆用鐵筋在爐炭上畫字筆談，寫完馬上壓平，像這樣慎重其事屏人密語的交談方式，或許有人認為故作姿態沒有必要，但唯有如此，秘密才能確保，不會輕易洩漏出去，有人說過：「當一個

人覺得保守秘密比洩漏秘密更為快樂時，這人真正成熟了。」大哉斯言。

此二則故事，告訴我們事無鉅細，一切以小心謹慎為上，特別是在對敵征戰時，更不可稍存有疏忽大意之心，清季中與名臣胡林翼曾說：「兵事不進則已，進則須策萬全」，又說：「用兵之道，全策為上」所謂萬全、全策，旨在強調任何細微末節都要注意不能輕忽，像這則發生在春秋時代之歷史故事，齊桓公與管仲謀伐莒，行動尚未展開，卻已先走漏了風聲，這是不是表示有什麼應注意而未注意之環節疏漏忽略了。齊桓公回憶當時情境，清楚的記得他與管仲在商議伐莒之初步計畫時，現場並無他人進出，何以消息會不逕而走頗感納悶，事後經瞭解得知原來係 1 名役人東郭郵，於服勤時偶爾抬頭看到齊桓公與管仲對談，根據兩人說話之唇形動作猜想而，所謂「口開而不闔」，加以手指方向，因而大膽的預測出將有伐莒之行動。

由上可知機密資料之掌握不一定完全依賴傳統之文書、會議或通信網路等資料才能獲取，純粹兩人之交談，僅憑雙方之口型及肢體動作，即能臆測出相關訊息，做出正確判斷。

因此我們公務人員平日處理公務時，除了必須要嚴格遵守各項保密規定，嚴防洩密情事外，任何細微末節都要注意，大意不得；至平時出入公眾場合，亦應謹守分寸，不探詢傳播公務，不談論公務行止，務要做到嚴絲密縫之保密要求，方策良全。

（以上資料摘錄自司法院政風處網站）