

• 稽核作為

本部及所屬機關98年資訊機密維護專案稽核執行重點摘述如下：

(一) 稽核對象：

本部及所屬機關之電腦使用者（含外包、廠商人員）。

(二) 稽核小組編組：

由本部及各所屬政風室、資訊室組成稽核小組，小組成員如下：

1.召集人：各機關政風室主管（綜理資訊安全稽核業務）。

2.副召集人：各機關資訊室主管。

3.組員：

(1) 資訊室電腦作業科長及資訊安全承辦人（執行稽核技術事項）。

(2) 政風室公務機密維護業務主管及承辦人（辦理資安稽核秘書作業）。

(三) 稽核方式與時間：

1.由「稽核小組」負責查核相關工作之執行情形，查核人員並得調閱有關資料、實地檢測資訊軟、硬體設備使用情形，並請相關資訊作業人員提供書面及口頭說明。

2.稽核編組人員視各單位使用資訊安全重要性，依據稽核表列項目進行實地稽核，並請受稽核單位指派相關人員提供相關資料說明。

• 稽核結果

(一) 一般資安稽核項目

本部及各所屬機關資訊機密維護專案稽核小組計稽查37個單位、58家代檢廠（公路總局高雄區監理所），自我評審表186人次，實地電腦稽核者計142件，相關稽核結果列述如下：

序號	缺失項目	說明	列為缺失之稽核機關	改進建議
1	個人密碼未定期更新	部分同仁常以更換密碼容易忘記為由，未能養成定期更新作業系統密碼之習慣、或設定之密碼長度不足、或將密碼以便利貼置放於電腦週遭，無法有效確保個人電腦使用安全。	高雄港務局 公路總局 交通部	請各單位同仁相互協助，另請各主管加強宣導，並要求同仁確實辦理。



廉潔正直
出於公而不染
廉潔正直
出於公而不染

法務部98年政風工作年報

2	安裝非法軟體或未經授權核准設定遠端監控功能之軟體相關設備	部分同仁為圖方便，對軟體版權不查、或因好奇而下載安裝不明相關軟體、或未能先行篩選相關項目即逕予全面安裝，造成影響系統執行速度。	高雄港務局 公路總局 交通部 基隆港務局	有關部分同仁因公務需要使用尚無版權之專業工具軟體，宜請各單位統計軟體需求數量，彙報由資訊室（人員）研議辦理採購事宜。
3	漏未使用螢幕保護加密設定，或使用無效設定	部分同仁未依「資訊安全政策」規定，開啟螢幕保護程式，或未設定密碼保護，或設定過長的靜置時間（如30分鐘），無法確實保護個人電腦資訊安全。	基隆港務局 高雄港務局 公路總局 交通部	請各單位同仁相互協助，另請各主管加強宣導，並要求同仁確實辦理。
4	未關閉電子郵件預覽功能	部分同仁為求便利，未關閉電子郵件預覽功能，或未設定以純文字閱讀。	基隆港務局 高雄港務局 公路總局 交通部	要求同仁正確使用電腦，關閉電腦電子郵件「預覽功能設定」，以避免遭到社交工程攻擊。
5	未開啓Windows自動更新功能	部分電腦未開啓Windows自動更新功能，致部分安全性更新程式未修補，易遭受資安「零時差攻擊」。	基隆港務局 高雄港務局	建議有關資訊安全規範及資訊設備異常通報系統等訊息，業刊登於各機關行政內網網站首頁頁面，請各同仁確實瀏覽閱讀，避免資訊危失態樣重複發生。
6	未安裝防毒軟體並隨時查看與防毒主機之連線狀況	部分電腦中發現大量疑似病毒之檔案。	高雄港務局	請資訊單位予檢查、刪除，並依規定安裝防毒軟體、Spyware Doctor間碟程式掃描軟體，以強化資通安全。
7	人力派遣人員之電腦設備未與機關內網系統作有效實體隔離	前次稽查發現○○工程顧問公司人力派遣常駐本局新工組協助審核工程設計案件之專業人員，其使用之電腦設備未與公路總局內網系統作有效之實體隔離。	公路總局	經協調該局資訊室妥處結果，除無法進入本局行政網站使用差勤系統外，亦無法進入本局公用資料區進行資料之存取及使用本局之資訊資源，已符行政院相關資安規定。
8	未取消資源共享功能		基隆港務局	建議有關資訊安全規範及資訊設備異常通報系統等訊息，業刊登於各機關行政內網網站首頁頁面，請各同仁確實瀏覽閱讀，避免資訊危失態樣重複發生。
9	不熟悉應用電子公文檔管理系統製作密件文件者作業流程		基隆港務局	
10	將重要公務檔案資料留置於電腦桌面		基隆港務局	
11	少部分電腦流量出現異常情形		基隆港務局	將不定期請各單位資訊室配合瞭解原因並設法向同仁宣導，加強注意。

(二) 社交攻擊演練

現目前研究顯示，駭客偏好利用「網路釣魚」手法滲透單位網路，成功機率高，使用者不易發現，風險不容輕忽。此種手法誘騙使用者受騙上當達到目的，一旦執行郵件中的惡意程式，或點閱、瀏覽惡意網站，是導致主機感染惡意程式的主要管道。輕者網頁遭到綁架，重者系統主機遭植入木馬或後門程式，造成機密資料或個人金融資料外

洩，造成嚴重損失。

本部為瞭解所屬機關同仁資安意識的落實狀況與對社交工程、網路釣魚等攻擊行為的防護能力，於98年依據行政院國家資通安全會報98年2月5日資安發字第0980100053號函檢送之「國家資通安全通報應變作業綱要」，辦理「交通部暨資安責任等級列A、B級所屬機關電子郵件社交攻擊演練」，演練結果簡述如下：

- 1.98年度目標：惡意郵件開啓率、點閱率分別降至16%及9%以下。
- 2.演練對象：本部暨所屬A、B級機關（不含事業機構），包括本部、中央氣象局、公路總局、飛航服務總臺、民用航空局桃園航空站等；此外尚有部分係自願參與演練者如台中港務局、基隆港務局、高雄港務局、運輸研究所、中華郵政股份有限公司。
- 3.第1次社交工程演練：達到演練目標的A、B級機關為中華郵政、運輸研究所、民用航空局桃園航空站、公路總局。
- 4.第2次社交工程演練：達到演練目標的A、B級機關為中華郵政、公路總局、飛航服務總臺、民用航空局桃園航空站、基隆港務局。

綜觀上述測試結果，顯示本部及部分所屬機關同仁對電子郵件安全認知仍有待加強。未來本部及所屬政風機構將配合法務部政風司的年度工作以辦理資訊安全宣導講習及資訊安全機密維護健檢，作為資訊安全業務重點工作。

• 結語

資通安全工作是長期、無止境的攻防與挑戰，本部及所屬機關資通安全管理規範日漸完備，然在相關管理面、教育訓練面有待持續落實與強化。為機先預防資訊危安事件，除強化系統工具協助管理外，最重要的就是考量人的因素（變數），此係現階段策進資訊安全的重要工作。

本部除持續落實資安管理與稽核作業外，本部及所屬政風機構仍將持續本於權責，協助機關制定完整且嚴謹之資通安全規範、強化內控機制、落實內部資訊稽核、加強辦理員工資訊安全認知之教育訓練及宣導，俾鞏固機關同仁之公務機密維護觀念，進而落實資訊安全工作，共同維護機關之資訊安全及民眾之權益。



出於淨而不染 濟世利生
出於淨而不染 濟世利生

§ 高雄市政府政風處查處洩密及違反保密規定案件研析

• 前言

隱私權係個人基本自由與權利，他人應予尊重，公務員執行公務時常有機會接觸民眾個人隱私或資料，本應依據相關法規嚴予保密，倘若發生公務機密資訊洩漏案件，將可能對相關當事人造成難以彌補之傷害。

高雄市政府推動各項市政，警政、戶役政、稅務、監理、環保、醫療等機關均掌握大量民眾個資，為深入探究洩密之原因與管道，以及違反保密規定之案件發生癥結，茲針對高雄市政府各機關於97、98年度所發生之洩密及違反保密規定案件，提出探討分析，切實掌握潛在之洩密風險，並研擬有效防範及管制措施，務求杜絕洩密案件發生，更臻落實公務機密資訊維護作為。

• 案件分析

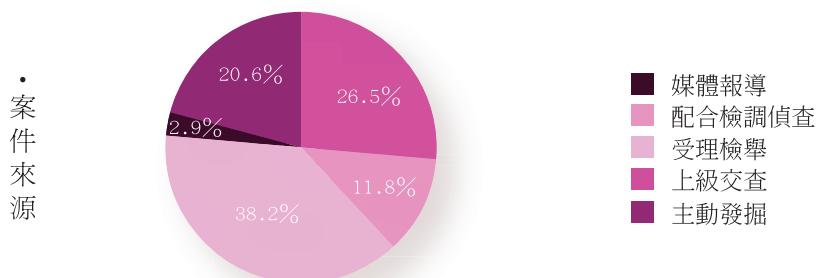
(一) 高雄市政府所屬各機關辦理97、98年度查處洩密及違反保密規定案件，總計34案，茲分就其發生機關、案件來源、洩密態樣、涉案人員及查處結果等項目，進行數據圖表分析如下：

1.依發生機關分析：

本期相關案件數量以發生機關區分，以警察局24件（70.6%）為最高，衛生局2件為次高，餘經濟發展局、環境保護局、研考會、勞工局、工務局、社會局、前鎮區公所及三民區公所均為1件。

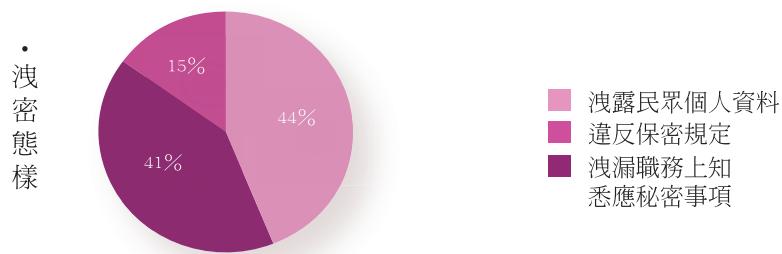
2.依案件來源分析：

案件來源係指洩密案件之發掘與獲得方式，其中上級交查9件；配合檢調偵查4件；受理檢舉13件；媒體報導1件；主動發掘7件。則上揭案件係受理民眾檢舉案件居多，其他是上級機關交辦案件，再其次則為主動發掘。



3.依洩密態樣分析：

洩密態樣乃指涉嫌洩密之型態，其中洩漏民眾個人資料案件15件；洩漏職務上知悉應秘密事項案件14件；違反保密規定案件5件。則上揭案件以洩漏民眾個資者居多，其次為洩漏職務上知悉應秘密事項。



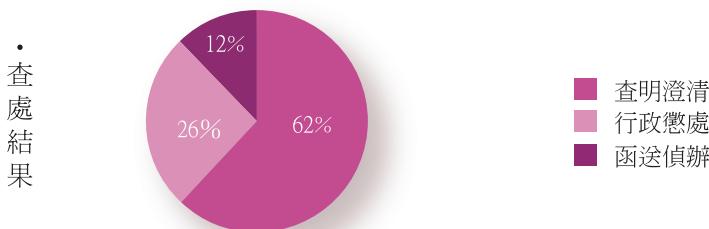
4.依涉案人員分析：

上揭洩密查處案件，除涉案人員無從特定者5案外，涉案人員共計38人，以職系區分，警職人員部分33人（86.8%）；非警職人員部分5人（13.2%）。查涉及洩密或違反保密規定案件之人員，係以第一線基層員警居多。



5.依查處結果分析：

上揭34件洩密案件，經查處結果做成之結案判斷：查明澄清21件；行政懲處9件；函送偵辦4件。





廉潔正直出於心而不染 證據由我出

法務部98年政風工作年報

- 本機關易滋洩密業務項目

茲就警政專屬業務及非警政專屬業務分以陳述：

(一) 警政專屬業務：

- 1.妨害風化營業、私娼、賭博電子遊藝場所及違規攤販佔道營業等取締事項。
- 2.犯罪偵防（重大刑案、治安人口、查捕逃犯、刑案資料）
- 3.戶口查察業務（戶役政資訊）。
- 4.特種勤務（含高層長官蒞臨場所與道路警衛）。
- 5.報案系統接收處理（報案三聯單）。

(二) 非警政專屬業務：

- 1.受理暨處理民眾舉發、陳情、檢舉事項。
 - 2.戶役政、稅務、監理、環保、醫療、社福等資料庫之運用暨管理。
 - 3.採購、人事、資訊等業務。
- 洩密（違規）案件類型及發生癥結

(一) 洩密（違規）案件類型：

綜觀上揭案件，依其案情內容大致可分為以下幾種類型：

1.洩漏民眾個人資料19件：

(1) 此類型為非警察機關發生8件。審究其因，少部分為承辦人員辦理民眾檢舉陳情案件未遵守相關保密規定，部分則為承辦機關與民眾認知不同或法規規範不明確所致。

(2) 此類型警察機關發生11件。員警非因公務查詢民眾個人資料（戶籍、車籍、刑案前科資料等）交予或告知他人知悉者，其原因大部分係受親朋好友請託幫忙查詢，少部分則係基於私務，利用職務之便，未依規定使用公務查詢系統，又未妥善保管查詢資料所致。

2.洩漏職務上知悉應秘密事項10件：

(1) 此類型警察機關發生9件、非警察機關（衛生局）發生1件。少數員警偵辦刑事案件時未嚴格遵守「偵查不公開」之規定，洩漏刑案偵查機密予媒體報導，導致犯罪嫌疑人及相關人的名譽、隱私或其它權利遭受侵害。再者警察機關之調查筆錄等公

務機密資料經由電腦網路外洩者不勝枚舉，而上開案件亦有數件機密資料經由網路外洩案件，雖並未發現承辦人之公務電腦有安裝P2P分享軟體，惟自網路發現機密資料外洩時至調查前，承辦人可能已將P2P軟體移除，致查無實證。抑或該機密資料係以未加密之電子郵件傳送其他相關承辦人知悉、存於私人隨身碟攜至他處使用，經駭客以木馬程式竊取，導致機密資料外洩。

- (2) 衛生局此案則為當事人不當運用所持有應秘密之採購案件資料，致生洩密之虞情形。

3.違反保密規定5件：

此部分警察機關佔4件，原因多為員警利用警政查詢系統漏未登記所致。

(二) 漏密（違規）案件發生癥結：

- 1.保密觀念不足或因自身警覺性不夠，無意間洩漏公務機密而不自知，例如：

- (1) 與朋友閒話家常時，內容談及工作情況，極有可能不經意地提及業務上應秘密之事項。
- (2) 下班或短暫離開辦公室時，未將機密文書收妥放置於辦公桌抽屜內或置於加鎖之公文櫃，致遭人窺探。
- (3) 公文製作、會辦，影印或傳真機敏資料時，因疏忽致機密資料外流。
- (4) 不諳相關陳情（檢舉）人身分保密規定，致使處理程序出現瑕疵，如發文時，檢舉人與受檢舉單位正副本並列等情。

- 2.警察機關電腦使用不當致調查筆錄、偵查報告等公務機密資料經由網路外洩事件層出不窮，究其原因臚述如下：

- (1) 任意將機密資料攜回家中使用私人電腦處理，極易遭駭客竊取而不自知。
- (2) 公務電腦任意下載安裝來源不明軟體或隨意開啓來源不明郵件或不當網站，致使電腦感染病毒甚至被植入木馬程式。
- (3) 個人電腦的帳號密碼未予妥善保管或資料查詢後未退出作業系統，使他人有機可乘。
- (4) 相關電腦知識不足，以P2P軟體為例，如使用者不知其分享功



廉潔奉公 不為私情所動
出淤泥而不染 濡清波而不染 廉潔奉公

能，即可能誤將機密資料予以分享外洩。

- (5) 以電子郵件傳送機密資料卻未加密，導致傳輸過程中機密資料遭駭客竊取。
- 3.地檢署、法院、調查局皆有規定，記者不得任由進出，故少有直接洩密之問題。但反觀各警察機關，卻讓記者自由進出刑事偵查部門，因而提高媒體記者直接拍攝到刑案偵查中相關人等照片或翻拍警方蒐證照片、影帶之機會，縱使事後經承辦員警以遵守偵查不公開原則要求記者不得刊載報導，仍無法避免偵查機密外洩。
- 4.警察機關單位主管對所屬同仁平時工作未能不定期勾稽掌握，或依規定逐日逐筆核對電腦查詢資料，機先發覺異狀，即時處理防範，尤其容易輕忽品德欠佳人員利用職務之便，使用相關查詢個人資料作業系統不法查詢或洩漏民眾個人資料。

- 強化公務機密維護措施之建議事項

(一) 法規面：

- 1.鑑於公務機關所保管之個人資料種類繁多，實無法逐一羅列，為避免有所闕漏，法務部制定之「個人資料保護法」已完成三讀，經總統公布，擴大原「電腦處理個人資料保護法」保護範圍，惟部分條文尚未生效，宜儘速訂定該法施行細則並施行，以使民眾權益之保護更臻周延。
- 2.警政方面，中央政府宜邀集警政單位、學者、新聞媒體代表、新聞評議單位或社會公正人士，共同制定「新聞採訪公約」，對於不同類型的犯罪偵查案件，訂定各類發布要點，尤其對於案件偵查進度及內容也應有不同程度的公布規範。如此，除了保障人權之外，也能讓新聞媒體與警察機關之間建立一定的程度的共識與默契。

(二) 制度面：

1.全面落實檢舉（陳情）人身分保密制度

本期非警察機關之洩密案件，多與檢舉（陳情、舉發）人身分疑似洩漏有關。因此，為鼓勵民眾勇於檢舉，建立全民監督機制，並確保渠等權益不受侵害，應落實檢舉（陳情）人身分保密制度。