宜蘭縣員山鄉公所

公務機關洩密風險

防貪指引會議

公務機關洩密風險議題討論

類型一、健保署承辦人受他人教唆查詢資料案。

項次	標題	說　　明
1	類型	健保署承辦人受他人教唆查詢資料案。
2	案情概述	中央健保署承辦人甲，職司投保單位基本資料維護、加退保、薪調作業以及補充保費之收繳，為依法令從事於公共事務，而具有法定職務權限之公務員。 任職於A公司之乙教唆甲利用公務之機，查詢非業管單位B公司之資料，甲將B公司資料鍵入該署承保應用系統作業查詢該公司之在保人員丙等人資料，並將查詢所得畫面提供予乙。 嗣因乙不滿未通過適用期考核被丙通知辦理離職，而將前開查詢畫面發布於通訊軟體LINE群組內，足生損害於丙等人。 甲之行為已涉犯個人資料保護法公務機關違反特定目的蒐集、處理個人資料罪等刑事責任；有關行政責任部分，經服務機關以違反公務員服務法第6條移送，公務員懲戒委員會判決降壹級改敘之懲戒處分。
3	風險評估	(1)慫恿他人洩密同具可罰性 未具公務員身分者教唆他人犯罪，不僅未保守秘密之公務員具有刑事及行政責任，個人也難逃法律制裁。 (2)濫用法定職務權限 公務員於執行法定職務時，始具有查詢承保應用系統資料權限。逕自以社交、好奇或受

		他人教唆為由，違規登入電腦系統查詢與公務無關之個人資料，實已逾越法定職務權限。 (3)涉及公文書登載不實 公務員使用公務系統查詢資料應登載查詢事由，以供事後稽查，倘非基於公務理由而以不實事由登載於電腦系統，可能另涉犯刑法公文書不實登載罪。 (4)違反公務員保密義務 公務員服務法第 4 條第 1 項及刑法第 132 條第 1 項訂有保密義務相關規範，其中「應秘密」係指文書、圖畫、消息或物品等與國家政務或事物上具有利害關係而應保守之秘密者，不以具有明文規定為要。
4	防治措施	(1)界定資料查詢人員權限 公務系統存取權限，應限於執行公務必要者，對處理敏感性、機敏性資料人員，應依管理層級授予查詢權限，或依工作內容賦予存取權限，將承辦人所得查詢範圍限縮於與其業務相關聯者。 (2)深化公務機密維護觀念 機關承辦人員於處理有關民眾資料時，不得逾越法令規範，避免因資料之洩漏影響民眾權益，進而損及機關聲譽。 (3)建立資訊系統定期複核機制 本案係以「公務機關相關業務」為由查詢民眾個資，應透過納保作業系統定期稽核，查察異常徵候及缺失，進而建立機關內部控制

		制度及標準作業程序。
5	參考法令	(1)刑法第 29 條。 (2)刑法第 132 條。 (3)個人資料保護法第 15 條。 (4)個人資料保護法第 20 條。 (5)個人資料保護法第 41 條。

類型二 員警掩飾洩密，不實登載職務報告案。

項次	標題	說　　明
1	類型	員警掩飾洩密，不實登載職務報告案。
2	案情概述	某派出所員警甲上網瀏覽民眾乙在社群網站刊登與丙吵架之訊息，甲出於好奇心驅使，登入「M-POLICE」輸入丙之姓名，查詢丙國民身分證統一編號、出生年月日、戶籍等基本資料，復於同日以丙之身分證統一編號於該系統查詢丙之基本資料、刑案紀錄、駕籍、國人相片等個人資料。同日下午，乙與丙於PTT互傳訊息時，乙竟傳送「我的警察朋友告知我說你有前科，缺錢賣假貨，真是可憐」等內容。丙因疑己之個人資料遭人洩漏，遂向內政部警政署申訴。 案經該警察局函請分局協助調查甲上開查詢丙個人資料之原因時，甲為避免自己非因公查詢民眾個人資料遭懲處，竟基於公文書登載不實之犯意，於職務報告登載查詢原因為「職於該時段擔服巡邏勤務，依規定簽巡邏轄內金融機構，並盤查人車，行經巡邏線A路口，發現一女子行跡可疑，遂以M-POLICE查詢渠資料。職查詢渠身分證號基本資料，因發現M-POLICE頁面有該女子刑案資料之提醒，故又點選渠前科素行、汽機車駕籍、相片、戶籍等，並未發現其他不法。職查詢係因公使用，有紀錄可稽。」等不實事項，並持之交由該分局所屬派出所警員陳核，足生損害於丙，及內政部警政署管理警用行動電腦資料查詢之正確性。

3	風險評估	(1)對偽造文書法規認識不足： 警察人員職司犯罪預防與偵查，應依法行事，竟因好奇心驅使，非因公務查詢被害人之個人基本資料；事後為免東窗事發，復於職務報告虛偽紀載不實之查詢事由，不僅侵害被害人隱私，更有違公務人員應依法行政之倫理準則。 (2)欠缺應保守職務秘密意識： 員警基於職務經常查詢使用警用系統查詢戶籍、車籍等個人資料，致洩密敏感度降低；資訊科技流通快速，且具有不可回復性，易因一時輕忽造成嚴重後果，避免人為因素所生洩密，使用涉及個人資料查調系統時，應提高警覺，防範資料外洩。 (3)因職務查詢之便衍生犯罪： 員警具有登入內政部警政署警用行動電腦「M-POLICE」查詢資料之權限，卻於調查時製作登載不實之職務報告，涉犯公務員登載不實而誤觸刑法偽造文書罪。 (4)同仁心存僥倖便宜行事 機關尚無檢視所屬同仁有無確實依照各項規定流程執行公務機制，對於易滋基弊端業務亦未落實內部稽核，同仁易因此心存僥倖而便宜行事。
4	防治措施	(1)強化資通系統使用安全稽核 公務機關偽造文書案件多與非因公查詢有關，彰顯資通訊安全保密重要性，除事前預防，事後稽核檢查亦屬重要。應藉由定期或

		不定期稽核，持續提醒同仁嚴守機關資通安全規定、電腦使用管理要點等作業規定，避免違失再生。 (2)加強法紀教育宣導，增進法規意識 應積極強化機關同仁正確之道德品操及價值觀，適時利用各種集會宣導貪污治罪條例、刑法偽造文書及妨害秘密罪章，或透過講習及教育訓練之舉辦，強化法規意識。 (3)提升資安觀念及保密意識 使用即時通訊軟體，應避免傳送涉及機敏性資料，自工作取得之訊息、文件、資料或刊物，若未經許可，不得洩漏、張貼、傳播或以其他方式散布。機關應持續利用各項機會場合宣導資訊安全管理規定、洩密違規案例及導致洩密管道與因素，建立同仁正確保密觀念，落實公務機密維護。 (4)落實風險控管預警機制 針對易滋生弊端業務，應持續要求並落實查察，各級主管對屬員應詳實考核，如有違法或違紀顧慮應即提報列管，必要時調整職務，以防衍生風紀問題。
5	參考法令	(1)刑法第 132 條。 (2)公務員服務法第 4 條。 (3)公務員服務法第 5 條。 (4)警察機關資通安全實施規定。 (5)警用行動電腦使用管理要點。

類型三、未諳採購法令規定，違法洩漏採購評選委員名單案。

項次	標題	說　　明
1	類型	未諳採購法令規定，違法洩漏採購評選委員名單案。
2	案情概述	機關承辦人員甲辦理採購案，以電子郵件洽詢該採購案各外聘評選委員是否有意願參加評選會議時，疏未注意而未將各外聘委員列為密件收件人，致各外聘評選委員收到電子郵件時即可得知其他評選委員姓名，因而涉違洩漏國防以外應秘密之消息。 案經轄區地檢署偵辦，以刑法第 132 條 2 項過失洩漏國防以外秘密罪，且事後坦承犯行，參酌刑法第 57 條所列事項及公共利益之維護，認以緩起訴為當，並命甲向國庫支付新台幣 1 萬元。
3	風險評估	(1)未諳政府採購法保密規定 承辦人員於尚在洽詢階段，未諳政府採購法令規定因而疏誤使評審委員名單外洩，觸犯刑法洩密罪。 (2)貪圖作業方便，致生廉政風險 機關承辦人員未熟稔電子郵件等寄發操作要領，疏未察覺評審委員名單應於上網公開前保密規定，為求作業方便竟以一次性電子信件同步寄發予多位評審，致使名單提早外洩。 (3)檔案管理不周，欠缺保密警覺 疏未留意採購案簽核公文、與各評審委員電話聯繫或書面文件往來過程皆屬職務上應保

		密事項，平日警覺性不足而忽略保密要領。 (4)社交工程演練，內控能量不足 以電子郵件遞送電腦病毒或後門程式亦可能導致機關資安事件，倘未積極辦理社交工程演練，極易致使同仁保密意識不足，未經深思熟慮及發送電子郵件，衍生洩密等不法事件。
4	防治措施	(1)辦理政府採購法令教育訓練 為增加得標成功率，競爭廠商間屢有透過管道於開標前獲取相關招標資訊情事，例如，投標廠商、評選委員名單等。為深化同仁政府採購法令認知，應強化相關法規宣導，將採購洩密違失納入教育訓練內容，建立採購人員倫理法治觀念。 (2)熟稔電腦操作要領 承辦人員應定期接受資訊教育訓練，若須以電子郵件洽辦採購案件，遇有群組信件，可將寄送之名單置於「密件副本」，使其他收件人無法同步得知，避免應秘密事項提前外洩。 (3)加強機關資訊安全社交工程演練 藉由定期及不定期資安工程演練，落實「停」(取消郵件預覽功能)、「看」(注意郵件主旨是否與業務相關）、「聽」(若懷疑郵件來源，透過電話向寄件知確認真偽)，避免開啟來路不明郵件，降低資料外洩風險。 (4)落實收(發)文、檔管公務機密檢查

		機密文書發文時應雙稿或分旨分文方式辦理，並於函覆時隱匿足資辨識委員身分之資訊，機關同仁於公文辦理時應落實文書保密規定，確保名單不外洩。 (5)建置機關採購作業內控程序 應針對工程、財物及勞務等不同類型採購，規劃採購作業標準流程圖或編撰範例，藉由作業流程之擬訂，避免同仁因不熟悉採購法令，或便宜行事逕援用錯誤前例，衍生採購洩密事件。
5	參考法令	(1)刑法第 132 條第 2 項。 (2)政府採購法第 94 條 2 項、採購評選委員會組織準則第 6 條第 1 項。 (3)採購人員倫理準則第 7 條第 1 項第 7 款。

類型四、利用職務機會洩漏地籍資料予工商徵信公司。

項次	標題	說　　明
1	類型	利用職務機會洩漏地籍資料予工商徵信公司。
2	案情概述	某縣市地政事務所地籍倉庫管理員甲，掌管地籍資料之管理、維護及報表製作，利用職務上得調閱地籍資料權限之機會，替工商徵信公司丙調閱不特定人之姓名、國民身分證字號，進而以該資訊查詢不特定人名下土地及建物之消息及謄本，並與該公司約定每案之查詢由丙依約給付新台幣600元。 甲為圖該公司應允給付之報酬，同意共同合作，遂基於對於主管地籍資料之事務，代為查詢應秘密之個人資料。
3	風險評估	(1)層級節制不足 承辦人員利用職務上機會，查詢得知不特定人所有之土地及建物消息及謄本。地籍資料之調閱欠缺內部主管之核准。 (2)監督機制欠佳 地籍倉庫管理員地籍資料之調閱業務抽查機制未落實，無法達到事前預警及事後追蹤目的。 (3)相關法治觀念薄弱 對於公務員保密義務及個人資料保護相關之法治觀念薄弱，不瞭解公務員洩漏職務上應秘密事項除刑事責任外，另將遭受行政懲處與公務員懲戒，嚴重者將喪失公務員身分。

4	防治措施	(1)強化主管督導作為 單位主管應落實承辦人員平時考核，知悉其平日人際交往情形，強化違紀人員考核作為，導正偏差之觀念，機先防處。 (2)資訊系統定期複核 機敏性資料之查詢應出於公務目的者，並以輸入承辦案件文號或查詢事由為要。應建立使用紀錄查核事宜等勾稽機制，對確屬異常者，核予行政責任。 (3)強化法紀教育宣導 利用各項集會機會，賡續辦理法治教育訓練持續加強宣導個人資料保護、公務機密維護之相關規定，藉由重申查詢應與職務具關聯性，防杜違法違紀情事發生。 (4)落實進出庫房簿冊欄位之登載 為利檔案管理人員地籍資料之管理，建議落實檔案資料庫房進出管控，避免管理違失所生洩密事件。
5	參考法令	(1)檔案法及其施行細則。 (2)刑法第 132 條。

類型五、機關資料庫遭駭客攻擊案。

項次	標題	說　　明
1	類型	機關資料庫遭駭客攻擊案。
2	案情概述	110 年 6 月某部會所屬基金會(資安 A 級機關)發生駭客入侵事件，受此事件影響者計該基金會所轄「新新聞片庫」等 9 大系統。 該案案緣機關人員於發現系統異常通報內部高階主管後，進行盤點檢查，因而查悉不法人士係以兩種病毒進行加密勒索攻擊，並要求支付比特幣。經資安廠商為檢查中之主機進行隔離、掃描、排除作業。該基金會找出一隻加密勒索攻擊之檔案即模式，提交資安廠商進行處理。 該勒索病毒攻擊事件根因於相關場域關鍵基礎設施使用者未落實「資訊安全管理制度(ISMS)」相關程序書、標準書之規定，有私自接用網路設備上網等資通安全防護漏洞，致發生上揭網路遭勒索病毒攻擊事件。
3	風險評估	(1)電腦作業系統老舊 機關大部分電腦作業系統均能更新至最新版本，但仍有部分公務使用之系統平台受限於軟體開發而無法更新。未更新之作業平台與軟體失去安全性，成為機關資通安全之隱憂。 (2)使用者習慣不佳 安裝來路不明程式、隨意點選瀏覽網頁或連結、不當使用電子郵件、擅自更改系統環境設定或使用私人資訊設備等，均可能造成機

		關資通安全疑慮。
4	防治措施	(1)慎選遠端連線工具 除微軟內建的遠端桌面功能，仍有許多軟體可提供遠端連線服務，如有遠端連線需求，應慎選無資安疑慮之連線軟體，並依機關資安規定進行設定，以免駭客入侵。 (2)隨時保持系統更新 不論係使用何種作業系統，建議電腦按時配合軟體更新，藉由漏洞之修補維持系統處於最新狀態，且切勿自行關閉自動更新程式，以免駭客依循系統漏洞入侵。 (3)開啟防火牆且安裝防毒軟體 開啟內建防火牆避免外部攻擊入侵個人電腦；安裝防毒軟體並定期更新病毒碼，網路文件之下載應先進行掃毒，勿任意開啟。 (4)強化重要資料之備份 日常應進行重要資料之備份，預防惡意軟體或勒索病毒，即使電腦遭勒索病毒感染或上鎖，藉由資料備及還原，亦能確保重要資料之恢復。
5	參考法令	(1) 資通安全管理法。 (2) 資通安全事件通報及應變辦法。