花蓮縣地方稅務局-
111年公務機密維護（洩密篇）指引

案例一　違法查詢戶籍資料抵償借貸利息

案情摘要

A為OO稅務局稅務員，職務上有權查閱民眾之稅籍資料，因理財不善投資失利乃向B經營之地下錢莊進行借貸，而後因利息過高無法支付，B便要求A以查詢錢莊倒帳客戶之戶籍資料供其催討債務使用，以抵償遲繳利息。因此先由B將倒帳之借款人或其家屬之姓名、身分證號碼等簡要資料交由A，再由A以其公務上配有之電腦系統帳號、密碼進入戶役政資訊系統查詢提供，至案發共計洩漏10多筆個人資料。

風險評估

(一)法治觀念薄弱

A身為稅務員，無視蒐集民眾個人資料需基於公務目的、對於納稅義務人個人財產資料有保護義務等規定，因個人債務問題擅自違法查調民眾個資並交付地下錢莊供催討債務使用，其行為恐有觸犯刑法洩密罪及違反個人資料保護法等規定 。

(二)涉嫌公文書登載不實

基於內控機制，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，非基於公務理由而以不實之事由登載於電腦系統，該行為可能另涉及刑法第213條公文書不實登載罪。

(三)違反公務員保密義務

公務員服務法第4條第1項規定：「公務員有絕對保守政府機關機密之義務，對於機密事件，無論是否主管事務，均不得洩漏；退職後亦同」；刑法第132條第1項訂有洩漏國防以外之秘密罪之構成要件，其中「應秘密」係指文書、圖畫、消息或物品等與國家政務或事務上具有利害關係而應保守之秘密者而言，自非以有明文規定為唯一標準。

(四)內控稽核機制存有漏洞

機關內部雖能針對相關資訊系統進行權限管控及資料查調進行一定比率之定期稽核機制，然稅務員A心存僥倖，利用職務之便透過機關相關資訊設備或程序，查到特定人士之個人資料，自認應不會被抽核發現，顯見機關內控稽核機制存有漏洞。

防治措施

(一)瞭解所屬員工生活狀況

建議各單位主管適時注意所屬員工私下家庭交友狀況及金錢往來情形，針對長期有債務問題或與特定職業過從甚密者，予以加強列管，降低因個人因素查詢及洩漏民眾個資之機關風險疑慮。

(二)加強廉政法令宣導及公務機密教育訓練

定期針對貪污治罪條例、刑法公務機密、個人資料保護法規範，辦理員工講習教育訓練，透過觀念梳理及不法案例說明等方式，建立機關員工保密警覺及強化恪遵法令的觀念，以利明確瞭解公務中取得應保密資料之範圍、處理及利用應注意之事項，落實公務人員依法行政原則並維護人民隱私權益。有效減少機關同仁因不諳法令而誤觸法網之弊端發生。

(三)專人負責管控發掘查詢異常紀錄

落實執行「資通安全政策」之要求，指定專人負責對於納稅義務人財產及稅籍資料網路使用者之申請、異動、註銷、密碼配賦及線上作業使用情形等加強管制，並由資訊單位建立查詢異常紀錄檔，定期統計列印報表供業務單位主管參考。

(四)強化內控資料查調稽核機制

機關應依內部控制制度及標準作業程序，針對查調資料加強稽核頻率及次數採定期、不定期內部稽核，產製清單核對，審視使用者帳號於各作業系統查詢次數、查詢原因、查詢日期及是否在勤等，由行政複核作業驗證例行操作過程有無缺失，檢視是否有異常情事，並就稽核結果缺失或建議事項，逕會相關科室，並請同仁進行說明及改善。如有異常使用情事，應進行追查，確屬異常者，應通報政風單位查明，違反規定查詢或使用，依相關法令究責。

參考法令

1. 貪污治罪條例第6條第1項第4款(圖利罪)
2. 刑法第132 條第1項（洩漏國防以外秘密罪）。
3. 個人資料保護法第41條（意圖為自己或第三人不法之利益或損害他人之利益，而違反第15條規定，足生損害於他人者。）
4. 個人資料保護法第15 條（公務機關對個人資料之蒐集及處理，除第6條第1項所規定資料外，應有特定目的，並符合下列情形之一者:一、執行法定職務必要範圍內。二、經當事人同意。三、對當事人權益無侵害。）

案例二　稅務員公器私用違規查調他人個資

案情摘要

A為OO稅務局稅務員，名下擁有兩棟房子，為添補家用故將其中一棟出租。某日，A因房租與承租人房客B發生糾紛，想要寄送存證信函給B，但並不知道B的戶籍地址，苦惱之際，腦筋突然想起因查核稅務案件之需要，可以透過戶役政系統查詢，於是利用上班期間使用戶役政系統，鍵入查調原因「欠稅清理」，並輸入B身分證字號，搜尋並取得B戶籍地址資料。後A按前揭戶籍地址，寄送私人存證信函予B，未料，此事遭B向機關政風單位檢舉。

風險評估

(一)法治觀念薄弱

A身為稅務人員，理應知曉蒐集人民個資需基於公務之目的，並妥善保護納稅義務人個人資料，卻基於個人因素擅自查調民眾個資，恐有觸犯刑法洩密罪及違反個人資料保護法等規定。

(二)涉嫌公文書登載不實

基於內控機制，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，非基於公務理由而以不實之事由登載於電腦系統，該行為可能另涉及刑法第213條公文書不實登載罪。

(三)違反公務員保密義務

公務員服務法第4條第1項規定：「公務員有絕對保守政府機關機密之義務，對於機密事件，無論是否主管事務，均不得洩漏；退職後亦同」；刑法第132條第1項訂有洩漏國防以外之秘密罪之構成要件，其中「應秘密」係指文書、圖畫、消息或物品等與國家政務或事務上具有利害關係而應保守之秘密者而言，自非以有明文規定為唯一標準。

(四)內控稽核機制存有漏洞

機關內部雖有針對相關資訊系統進行權限管控及資料查調進行一定比率之定期稽核機制，然稅務員A心存僥倖，利用職務之便透過機關相關資訊設備或程序，查到特定人士之個人資料，自認應不會被抽核發現，顯見機關內控稽核機制存有漏洞。

防治措施

(一)加強廉政法令宣導及公務機密教育訓練

定期針對貪污治罪條例、刑法公務機密、個人資料保護法規範，辦理員工講習教育訓練，透過觀念梳理及不法案例說明等方式，建立機關員工保密警覺及強化恪遵法令的觀念，以利明確瞭解公務中取得應保密資料之範圍、處理及利用應注意之事項，落實公務人員依法行政原則並維護人民隱私權益。有效減少機關同仁因不諳法令而誤觸法網之弊端發生。

(二)加強查調系統相關教育訓練

部分公務員發生洩漏案件，多因對系統操作及相關規定不瞭解所致，因此應重視查調系統及使用規範之教育訓練，使業務承辦人員知悉查詢及運用相關資訊，應限於有助於公務目的達成始可為之，以防止資訊不當使用或外洩情事。

(三)專人負責管控發掘查詢異常紀錄

落實執行「資通安全政策」之要求，指定專人負責對於納稅義務人財產及稅籍資料網路使用者之申請、異動、註銷、密碼配賦及線上作業使用情形等加強管制，並由資訊單位建立查詢異常紀錄檔，定期統計列印報表供業務單位主管參考。

(四)強化內控資料查調稽核機制

機關應依內部控制制度及標準作業程序，針對查調資料加強稽核頻率及次數採定期、不定期內部稽核，產製清單核對，審視使用者帳號於各作業系統查詢次數、查詢原因、查詢日期及是否在勤等，由行政複核作業驗證例行操作過程有無缺失，檢視是否有異常情事，並就稽核結果缺失或建議事項，逕會相關科室，並請同仁進行說明及改善。如有異常使用情事，應進行追查，確屬異常者，應通報政風單位查明，違反規定查詢或使用，依相關法令究責。

參考法令

1. 個人資料保護法第41條意圖為自己或第三人不法之利益或損害他人之利益，而違反第15條規定，足生損害於他人者。
2. 個人資料保護法第15條公務機關對個人資料之蒐集及處理，除第6條第1項所規定資料外，應有特定目的，並符合下列情形之一者: 一、執行法定職務必要範圍內。二、經當事人同意。三、對當事人權益無侵害。
3. 刑法第213條公文書不實登載罪。
4. 刑法第132條第1項洩漏國防以外秘密罪。

案例三　欠缺保密意識洩漏採購評選委員名單

案情摘要

OO機關承辦人員A為辦理採購案成立採購評選委員會，期間以電子郵件發送該採購案各外聘評選委員詢問是否有意願參加評選會議，竟疏於注意未將各外聘評選委員列為密件收件人，致各外聘評選委員收到該電子郵件時即可得知其他評選委員姓名。案經OO地檢署偵辦A涉犯刑法第132條第2項過失洩漏國防以外秘密罪，且事後坦承犯行，檢察官予以緩起訴，並命向國庫支付新臺幣1萬元。

風險評估

(一)採購承辦人員欠缺保密意識

依據採購評選委員會組織準則第 6 條規定「本委員會成立後，其委員名單應即公開於主管機關指定之資訊網站……。機關公開委員名單者，公開前應予保密；未公開者，於開始評選前應予保密。」承辦人員於尚在洽詢階段，除未諳政府採購法令規定又欠缺保密意識，疏忽致使評審委員名單外洩，觸犯刑法洩密罪。

(二)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(outlook等)等寄發操作要領，未察覺評審委員於上網公開前相關保密規定，貪圖作業方便竟以一次性電子信件同步寄發予多位評審委員洽詢，致使名單提早外洩。

(三)刑法洩密罪亦處罰過失行為：

按刑法第14條規定之過失係指雖非故意，但按其情節應注意並能注意而不注意者，或對於犯罪之事實，雖預見其能發生而確信其不發生者而言。刑法第12條第2項規定，過失行為之處罰，以有特別規定者為限。而現行洩漏國防以外秘密罪包含過失行為，因此即使非故意洩漏秘密，仍屬刑法課責的行為。

防治措施

(一)加強辦理政府採購法廉政教育訓練

公務員貪瀆案件不少以洩漏採購案件資訊為前端行為(例如洩漏採購評審委員名單得以先行賄賂)，因此機關應將採購法保密規定及採購洩密違失態樣納入採購法教育訓練，以建立採購人員正確的倫理法治觀念，以避免疏失再犯。

(二)承辦人員應熟稔電腦操作要項

機關承辦人應定期接受資訊教育訓練，熟稔相關電腦操作要領；若須以電子郵件洽辦採購案件，除使用公務機關配發電子郵件帳號外，對於具有機密或敏感性資訊之電子郵件應採用加密方式處理，以免發生誤送或洩漏應保守之秘密等狀況。若以群組信件可將寄送者名單置於「密件副本」，使其他收件人不可同步得知，防範採購保密事項於上網公告前提前外洩。

(三)加強公務機密稽核

機密文書應雙稿或分旨分文方式辦理，並於函文時隱匿足以辨識身分之資訊，各級主管於公文核稿時亦應落實文書保密規定，以確保個資不外洩。對於電子郵件寄送，應採「密件副本」方式處理，應列入平時資安稽核或公務機密檢查項目，提醒同仁注意。

(四)落實採購人員平時考核，防杜洩密違失

各機關單位主管除應落實平時考核工作外，尚可透過首長信箱、問卷調查、訪查等多元管道，瞭解經辦採購人員之服務態度，並從中查察相關異常情形。查有違反相關規定者，應即時簽報機關首長予以調整職務，機先防範採購洩密違失情事發生。

(五)執行機關資訊安全定期稽核作業

為機先發掘資安漏洞，機關應定期、不定期或遇有重大洩密案件時，執行資安稽核或保密檢查，除改善缺失漏洞並提高防火牆功能以防駭客入侵外，同時藉此對執行良好者從優獎勵，對執行不力者依規定懲處，以導正機關同仁建立機密資訊維護的正確認知。

參考法令

1. 刑法第 132 條第 2 項過失洩漏國防以外秘密罪。
2. 政府採購法第 94 條第 2 項、採購評選委員會組織準則第 6 條第 1 項規定，「本委員會成立後，其委員名單應即公開於主管機關指定之資訊網站；委員名單有變更或補充者，亦同。但經機關衡酌個案特性及實際需要，有不予公開之必要者，不在此限。機關公開委員名單者，公開前應予保密；未公開者，於開始評選前應予保密。」（中華民國107年8月8日行政院公共工程委員會工程企字第10700240070號令修正發布）

   註:
   本案發生時間點適用採購評選委員會組織準則第6條舊法「本委員會委員名單，於開始評選前應予保密。但經本委員會全體委員同意於招標文件中公告委員名單者，不在此限。本委員會委員名單，於評選出優勝廠商或最有利標後，應予解密；其經評選而無法評選出優勝廠商或最有利標致廢標者，亦同。」
3. 採購人員倫理準則第 7 條第 1 項第 7 款：採購人員不得有下列行為：(七)洩漏應保守秘密之採購資訊。

案例四　洩漏採購機密文件

案情摘要

A機關辦理工程採購招標過程，接獲廠商B以密件發函針對招標內容提出異議，認該規格及廠商資格有限制競爭情形，故要求A機關釋疑並進行更正。上開異議以密件分文予本案承辦人甲，甲雖知悉該函文涉及規格疑義亦屬密件，惟因認相關內容涉專業判斷，須徵詢他人意見，故隨即以手機拍攝該函文透過LINE傳送予投標廠商C之負責人乙，請其針對異議內容協助研擬回覆，因涉及採購洩密情事。後本案經檢舉，承辦人甲經法院判決犯刑法第132條第1項洩漏國防以外秘密罪，處有期徒刑貳月，緩刑貳年。

風險評估

(一) 公務員對洩密罪「過失」之規定缺乏認知，實務上常見便宜行事，致犯洩密的案例。

(二) 承辦人與特定投標廠商關係匪淺，招標階段接獲異議即委請廠商協助處理，衍生觸法危機。

(三) 無法針對涉專業之採購異議內容進行釋疑，故尋求非正式管道處理，程序不備致生洩密。

(四) 未認知外部事項(包括採購異議、民眾陳情檢舉)應遵守相關保密規定處理不當誤觸法網。

(五) 與特定廠商進行程序外接觸，可能引發程序公平性質疑，甚至發生程序違法問題。

防治措施

(一) 各單位辦理政府採購招標階段應儘量避免與廠商進行「非必要程序外接觸」藉此維持機關公平公正立場，避免民眾訾議。

(二) 針對外部反映事項，建立標準處理程序供同仁依循，杜絕程序不備觸法問題。

(三) 涉及高度專業判斷之採購案件，應配合組成「採購工作及審查小組」，邀請外聘專家協審，運用正式管道處理爭議，降低過失洩密風險機率。

(四) 適時透過宣導，辦理講習或運用各會議說明等方式，建立機密維護正確的法令及程序觀念。

參考法令

1. 刑法第132條第1項。
2. 政府採購法第34條。
3. 採購人員倫理準則第7條第7款。
4. 行政院所屬各機關處理人民陳情案件。
5. 行政程序法第47條 。
6. 機關採購工作及審查小組設置作業辦法第6條。

案例五　LINE群組轉貼民眾檢舉信洩漏陳情人個資

案情摘要

市政府OO處A員為機關首長指定的密件分文人員，某日於處理市政信箱分派之民眾檢舉信件時，明知市府陳情案件依規定皆不得透露陳情來源、民眾個資、案件編號等相關資料，市府保密要點中也明定，民眾以電子郵件或線上陳情系統陳情檢舉等，由機關首長或指定的密件人員分文，A員竟為分文時效，將內容截圖至科內群組，確認是否為該科業務，因一時不察，將分派的檢舉信，包含檢舉人個資、相關內容等，以文字複製貼上方式傳送到多達20人的LINE同事群組中告知此事，因而洩漏檢舉人個資予以非承辦人知悉。案經檢舉政風單位調查後移送地檢署偵辦，A涉犯刑法第132條第2項過失洩漏國防以外秘密罪，犯後坦承深表悔悟且無前科，檢察官偵結予以緩起訴，並命向國庫支付新臺幣3萬元。

風險評估

(一)處理檢舉案件屬應保密事項

公務員服務法概括規定公務員應嚴守保密義務，實際上是否洩密及是否有加重處罰，則散見於刑法及其他法律，而本案為受理民眾陳情書與相關個人資料，應屬公務機密範疇，受理陳情檢舉案件相關承辦人應深入瞭解處理過程每個環節之保密規定。此外，對於檢舉人身分之保密義務並不因檢舉案件處理完畢而免除，需格外留意。

(二)欠缺保密意識

市府相關規定及保密要點亦有明定，民眾陳情案件皆不得透露陳情來源、民眾個資、案件編號等相關資料，然A員不瞭解行政領域中關於受理陳情檢舉之相關細節規定，欠缺保密意識，便宜行事將所分派的檢舉信，包含檢舉人個資、相關內容等，傳送到LINE同事群組，此舉已觸犯刑法洩密罪。

(三)刑法洩密罪亦處罰過失行為

按刑法第14條規定之過失係指雖非故意，但按其情節應注意並能注意而不注意者，或對於犯罪之事實，雖預見其能發生而確信其不發生者而言。刑法第12條第2項規定，過失行為之處罰，以有特別規定者為限。而現行洩漏國防以外秘密罪包含過失行為，因此即使非故意洩漏秘密，仍屬刑法課責的行為。

防治措施

(一)審視陳情案件處理程序，強化機關組織分層審核措施

藉由本案受理陳情案件處理過程之洩密疏漏，重新審視受理陳情案件處理程序，檢討相關規範是否完備、案件受理程序是否妥適及符合規定，嚴密機關組織分層審核措施，使機關承辦人員有所依循，避免衍生洩密情事。

(二)落實保護檢舉(陳情)人措施

行政院及所屬各機關處理人民陳情案件要點第18點規定「人民陳情案件有保密之必要者，受理機關應予保密」，受理民眾檢舉違規違法之單位，應落實檢舉案件內容及檢舉人保護管控措施，避免因身分資料洩漏對檢舉人生命及財產安全造成危害。

(三)賡續加強公務機密維護宣導

民眾個人資料外洩的主因大部分皆屬人為因素，因此欲降低資料外洩的機率，最主要還是要從培養個人之保密觀念著手。機關應持續辦理教育訓練或例行性宣導，以現行法令規定、洩密違規（法）案例，以及可能導致洩密管道與因素，適時提醒員工關注切身法律問題，發揮宣導效果，避免發生類似洩漏檢舉人個資情事，肇致刑事、民事、行政責任追究。

參考法令

1. 行政程序法第170條第2項。
2. 行政院暨所屬各機關處理人民陳情案件要點第18點及第19點後段。
3. 行政院頒文書處理檔案管理手冊第48點。
4. 獎勵保護檢舉貪污瀆職辦法第10條前段。
5. 刑法第 132 條第2項。

案例六 通訊軟體遭駭客入侵案

案情摘要

據科技新報網路新聞刊載，LINE台灣總公司發現旗下用戶的相關內容遭到擷取，對象竟包括我國的府院、軍方、縣市長、政黨等相關人士，清查後共有100多人遭駭客鎖定並入侵，LINE隱私設定中用於保護訊息的進階加密功能「Letter Sealing」，預設都是開啟，事後調查卻都遭到關閉。LINE是台灣人最常使用的通訊軟體，容易成為不肖份子利用各種方式攻擊、詐騙。由於此次事件涉及府院高層人士，恐對國安造成重大威脅，國安單位經深入調查，將近期遭揭發的間諜軟體「飛馬」（Pegasus）列入，甚至不排除有內神通外鬼的可能性，也藉此提醒做好個人資安保護以防遭駭。不過，國安高層進一步表示，包括正副總統在內，從總統府到府院高層人士是有專用的通訊軟體，特別強化點對點加密等安全機制，國家等級資訊是以專用通訊軟體溝通，至於與親朋好友或個人聯繫才會使用到LINE，不會用來傳遞政府機關的重要文件。

風險評估

(一) 資安威脅與日俱增

智慧型手機與平板電腦有助提升生活的便利性及行動辦公環境的生產力與效率，但使用者往往過度關注便利性及實用性，欠缺資安風險意識，忽略駭客常利用惡意

App盜取手機上的重要資料、監看用戶行為、製造詐騙廣告點擊或訂閱詐騙，也可能使行動裝置成為入侵其他裝置或資料庫的跳板。

(二)隱私權保護不易

雖然大眾對於隱私權保護的意識相較過去已大幅提升，但社群軟體及通訊軟體早已滲透個人生活中，企業利用使用者未意識之情況下不斷蒐集個人資料數據及資料分析技術，引發侵犯隱私權的疑慮，使用者勢必在安全、隱私及便利性之間有所取捨。

防治措施

(一)不安裝來源不明手機軟體

惡意應用程式已是智慧型手機的主要威脅之一，即使是在Google Play或App Store上架的應用程式亦可能暗藏惡意程式，而Android系統更可下載apk檔案自行安裝，面對App的資安威脅程度更高，因此用戶僅可從可靠信任的來源安裝App應用程式。

(二)不使用來源不明之公共(免費)Wi-Fi

目前國人使用行動裝置的比例越來越高，除了個人行動上網之外，免費無線網路熱點服務的範圍也十分廣泛，而駭客正可利用提供不安全的免費WiFi，竊取所有使用者連上該WiFi所傳送的資料，或是使用假網頁竊取輸入的帳號密碼，所以行動裝置應避免使用來源不明免費的公共熱點Wi-Fi。

(三)注意軟體使用權限

行動裝置上的軟體在安裝或在第一次使用時，多會詢問可獲取的權限，如讀取位置、儲存、聯絡人、相機、麥克風等，因此在安裝軟體時，宜注意該軟體是否要求不必要的權限，評估要求權限是否合理，再考慮是否進行安裝使用。

(四)慎選行動裝置硬體

我國禁止公務用之資通產品使用大陸廠牌，而在個人通訊設備上，亦應審選廠牌，國內曾發生某電信商販售的廠牌手機內建軟體內藏惡意程式，使用戶淪為詐騙集團人頭的案例。

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 。