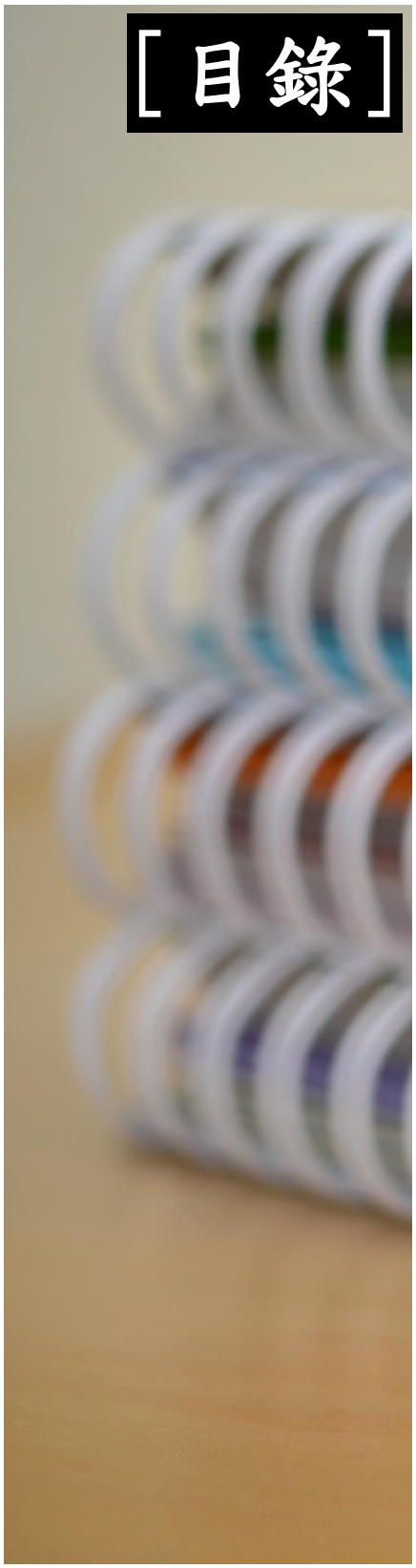


[目錄]

[前言]

在後疫情時代，居家辦公或是遠端作業，可能成為未來的工作型態之一，科技技術雖帶來觸手可及的便利性，卻同時隱藏著讓人容易忽視的資安風險，倘若對於資安意識不夠重視，在享受科技便利性的同時，伴隨而至的就將是造成機關資訊安全的破口。

政風單位秉持著協助機關安全防護與公務機密維護職責，深知面對資安威脅並非專屬於資通安全專職人員的工作，亦是機關內每一位同仁的責任，因此以加強深化同仁對於資訊安全的認知為目標，聚焦一般使用者面向，收集分析實務上發生之各種缺失態樣與防治措施，藉由編撰資訊使用管理安全防貪指引，提供同仁參考運用，以他山之石，引以為鑒，集眾人之力做好風險管理以杜絕可能危害機關或洩密的情事發生，確實維護機關資訊安全並保障民眾相關權益。

［不當查詢態様］

［案例1：公務員偷查並洩漏他人個資案］

甲係內政部移民署○○大隊科員，負責入出國（境）證照查驗、鑑識及許可、國境線入出國安全管制及面談之執行等入出境管理事務。詎其因與乙喜歡同一位女生，竟基於洩漏國防以外應秘密之犯意，利用公務電腦設備，以「入出國查驗系統」，輸入乙之國民身分證統一編號，查詢並蒐集含有乙統編、姓名、出生日期、出生別、役別、出生地、婚姻狀況、戶籍地址、軍種、體位、退伍令字號及退伍日期之「個人役政資料」，並以行動電話拍攝「個人役政資料」畫面後，藉由通訊軟體LINE傳送洩漏予第三人。後甲向法務部廉政署自首上情，經法院判處有期徒刑6月，如易科罰金，以新臺幣1,000元折算1日。緩刑4年，並向公庫支付新臺幣10萬元。

（參考資料：臺灣桃園地方法院109年度審訴字第1019號判決、臺灣高等法院109年度上訴字第3417號刑事判決、懲戒法院懲戒法庭110年度清字第1號懲戒判決）

風險評估	1、濫用法定職務權限： 依法令服務於國家所屬機關而具有法定職務權限之公務員，於執行法定職務時，始擁使用查詢入出境紀錄及戶役政資料之權限，且依「內政部移民署使用戶役政資訊系統作業管理要點」之規定，戶役政資料之查詢及運用，應以辦理入出境管理及移民署業務需要者為限。然而公務員基於社交或好奇為由，違規登入電腦系統查詢與公務無關之個人資料，逾越法律賦予之職務權限，造成行政濫權。 2、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，因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。 3、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(最高法院91年度台上字第3388號刑事判決)。
防治措施	1、公務機密教育訓練： 保密係公務員應盡義務之一，機關應針對同仁進行公務機密教育訓練及宣導，以利同仁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，並遵守保密義務，落實公務人員依法行政原則並維護人民隱私權益。 2、資訊系統定期複核： 機關應依內部控制制度及標準作業程序採行內部稽核，由行政複核作業驗證例行操作過程有無缺失，並就稽核結果評估監控機制之有效性。本案係以「公務機關相關業務」為由查詢民眾個資，如與民眾實際出入境資料相互勾稽，即可發現公務員查詢個資時間與民眾出入境時間未符，甚至無出入境紀錄，行為即具異常徵候。
參考法令	1、刑法第132條 2、個人資料保護法第19條 3、個人資料保護法第20條

［案例2：受他人教唆查詢資料案］

甲任職於中央健康保險署○○業務組之業務助理，以承辦投保單位基本資料維護、加退保、薪調作業及補充保費之收繳為其業務，為依法令從事於公共事務，而具有法定職務權限之公務員。乙任職於○○公司，教唆姑姑甲利用公務查詢非業管單位之○○公司資料，甲將○○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佈於通訊軟體LINE群組內，足生損害於丙等人。經法院判決甲犯個人資料保護法第41條之公務機關違反特定目的蒐集、處理個人資料罪，處有期徒刑2月，如易科罰金，以新臺幣1,000元折算1日。緩刑2年，並應於本判決確定後6個月內向被害人丙支付新臺幣3萬元之損害賠償。

（參考資料：臺灣士林地方法院107年度審簡字第78號刑事判決）

風險評估	1、慫恿他人洩密同具可罰性： 教唆他人使之實行犯罪行為者，為教唆犯。因身分或其他特定關係成立之罪，其共同實行、教唆或幫助者，雖無特定關係，仍以正犯或共犯論。刑法第29條及第31條分別訂有教唆犯及共犯規定。未具公務員身分之人濫用親情慫恿他人犯罪，累及親屬，不僅未守保密義務之公務員應受苛責，個人也難逃法律制裁。 2、侵害個資需負擔賠償責任： 公務機關違反個人資料保護法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。若被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣500元以上2萬元以下計算。
防治措	1、劃分資料查詢人員權限： 公務系統存取權限，應以執行公務必要者為限，對處理敏感性、機密性資料之人員，應依不同管理層級分別授予查詢權限，審視人員工作內容賦予存取權限，負責特

施	定轄區業務範圍之承辦人限縮查詢該業務轄區之權限，妥適分工分散權責並建立評估及考核制度，及建立代理人互相支援制度。 2、建立維護公務機密觀念： 公務員處理公務，大多與民眾權益相關，行政措施均不能逾越法令規定範圍，且公務員負有保守公務機密之義務，刑法上有制裁規定，不單純行政懲處為已足。因此公務機關各業務承辦人員平日應時刻提醒自己隨時檢點個人言行，在處理有關民眾資料時，應更加嚴謹，以防因資料之洩漏而影響民眾之權益而受罰，或影響機關之聲譽。
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

［案例3：法官公器私用濫用查詢系統案］

臺灣○○地方法院法官甲職司審判業務而經司法院配發戶役政電子閘門系統識別碼（即個人帳號）及密碼，詎甲自99年11月24日起迄至100年9月2日止之任職期間，因申報財產、報稅及為次子命名參考等用途，使用戶役政電子閘門系統，以輸入其承辦案件案號，或輸入非承辦案件案號等方式，查詢與其承辦案件無關之自己祖母、父、母、岳父、胞姊及長子等之個資，並輸入預想虛擬之姓名查詢以作為其即將出生之次子命名之參考，其中部分人名確有其人存在。其行為經政風室稽核發現，嗣經司法院人事審議委員會審議，建議處分記過2次。

（參考資料：法官評鑑委員會評鑑決議書101年度評字第4號）

風險評估	1、未詳實鍵入查詢案由： 行為人於接受評鑑時指稱系統查詢流程繁瑣，重新查詢其他案號時，均要重新輸入年度、字號別、案號數字等3個欄位，或是系統閒置過久清空原輸入欄位等理由，輸入任意案號或「000」等空白案號，未輸入自己承辦案件之正確案號。 2、間接侵害他人隱私： 行為人為即將出生之子女預想命名，於戶政系統內輸入自己設想之虛擬姓名作為參考，但其中部分姓名確有其人存在，雖行為人於真實生活上不見得認識其人，但查詢資料非作為公務使用，隨意探視他人個資，仍屬間接侵及他人隱私。 3、漠視資安規定： 司法人員應公正廉明、守法盡職，卻僅以報稅、財產申報、測試系統資料更新速度及為子命名等理由，隨意鍵入他人姓名查詢，並認為只要無用以營利而可說明用途等情即可，無意識此等行為已屬違規之舉。
防治措	1、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，使公務員知悉查詢及運用相關資訊，應限於有助於

施	公務目的達成始可為之，以防止資訊不當使用或外洩情事。 2、定期稽核資訊系統篩選異常： 任何查詢涉及機密性資料均應輸入承辦案件之文號或查詢事由，作為日後查核之依據。機關內部應設立查核單位負責使用記錄查核事宜，如有異常使用嫌疑，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，依相關法令負責。
參考法令	1、司法院暨所屬各機關使用識別碼及密碼查詢院內網路資料作業注意要點第4點 2、司法院及所屬各機關資訊安全管理要點第30點 3、司法院暨所屬各機關使用對外連線資料管理要點第4點 4、司法院及所屬各機關使用戶役政資料管理要點第4點 5、司法院及所屬各機關使用戶役政資料管理要點第6點

［案例4：警備隊員私查上千筆個資案］

據報載，○○市一名負責總統官邸維安的警員，平時使用警用小電腦清查來往可疑車輛，某次遇到同單位女警脫口說出其住家地址，私查個資的行為才因此露餡。經警局內部清查發現該警員假公濟私利用警用電腦調閱上千筆個資，對象從分局長到分局女警、僱員、工友等，清查過濾後發現查閱對象資料並非工作所需。警局得知該員不當使用電腦查詢資料，但尚查無洩密或不當使用，已進行行政處分並調離原單位，同時停止電腦使用權限。

（參考資料：蘋果日報新聞）

風險評估	1、資安價值觀念偏差： 警務人員依法執行職務，具有查證身分、鑑識身分、蒐集資料，甚至施予直接強制等公權力權限，如個人資安意識不足，可能造成個人價值觀偏差，加上存有僥倖心理便宜行事，即有可能以身試法，致衍生風紀問題。實務上亦曾發生警員因好奇心作祟濫查名人、政府官員或地方民代個資案例發生。 2、機關漠視高風險人員： 警務人員因執勤及維護治安所需，利用M-Police系統串接至眾多政府資料庫，提供第一線執勤人員線上查詢以辨識民眾資料，有效提升治安維護效能。惟甲於警局內部已有不當查詢個資以及超出正常查詢次數而受行政懲處前例，卻未將該員列為風險人員調離特殊勤務職位，以致該員得以持續在非職務狀況下，濫用職權查詢私人個資。 3、受他人請託查詢： 實務上常見基於人情請託或同事情誼，通過利誘或各種理由搪塞，如偵辦案件之急迫性或時效性，委請不知情同仁代為查詢資料，藉此方式違法取得利用他人資料，衍生違法洩密，破壞政府公信力及形象。
防治	1、嚴明律定使用時機： 警政資訊系統係提供警察同仁執行勤務或犯罪偵防時，能透過政府資料整合、分析、勾稽檢索功能，以有效快

措施	速取得個人資料，因此應嚴正聲明使用時機限於公務使用，違反查詢規定者應受責難 2、落實風險人員評估 機關應辨識可能造成機關內部危害之人員，如涉嫌不法、財務異常、風評不佳、行事作風違常迭遭檢舉之人員，提列為風險人員，落實平時考核，對其採取風險控制措施或擬具預警防範作為，強化監控密度。 3、帳號專人使用管理 有關系統查詢之個人帳號、密碼應妥為保管，不得借予他人使用或張貼於電腦設備等容易外洩環境。如因公務需求接受其他同仁委託查詢，應同時記載委託人員姓名、單位及事由，供日後查核使用。
參考法令	1、個人資料保護第5條 2、警用行動電腦使用管理要點第4點 3、警察機關資通安全實施規定第16點 4、內政部警政署戶役政資料電子閘門系統作業管理規定第5點 5、內政部警政署車籍資訊系統查詢作業規定第6點

[資訊外洩態樣]

［案例5：公務員期約收賄販賣個資案］

甲擔任○○縣警察局刑事警察大隊偵查佐，負責刑事案件偵辦工作，並因公務需要而有向各電信業者調閱電話申登人資料、通聯紀錄之權限。乙受徵信業者委託，透過有權限查詢個人資料之公務員取得個人資料並販賣之。甲、乙均明知非因案件偵辦需要，員警不得查詢電話申登資料及通聯紀錄進而提供業者使用，乙基於期約賄賂之意思，向甲提議調取通聯單向1日3,000元、雙向1日6,000元、通聯單向3日6,000元、通聯雙向3日1萬2,000元之價格，對於查詢個人資料並洩密之行為，期約給付甲上開報酬，而甲則基於期約賄賂之意思，允諾為乙蒐集個人資料。經法院一審認定甲對於違背職務之行為，期約賄賂；洩漏國防以外應秘密；行使登載不實公文罪，應執行有期徒刑12年。上訴二審改判洩漏國防以外之秘密消息罪，處有期徒刑3月，如易科罰金，以新臺幣1,000元折算1日；又犯行使公務員登載不實文書罪，處有期徒刑1年6月。違背職務之行為期約賄賂部分無罪。

（參考資料：臺灣臺北地方法院99年度訴字第47號刑事判決、臺灣高等法院101年度上訴字第143號刑事判決）。

風險評估	1、警察機關容易取得個人資料： 警務人員因職務內容特殊，取得民眾個資之管道十分容易，又因於執行警察各種任務之範圍事務內經常使用民眾個資，因此對於持有個資乙事習以為常，可能因此降低對於持有公務機密與個資保護之敏感度。 2、組織犯罪的可能性： 近期仍有不肖員警將個人資料販售予徵信業者不當利用的案例，亦有不法集團販賣個資給詐騙集團之案件發生，足見個人資料之洩漏及遭濫用之嚴重程度，而大規模資料外洩更容易招致個人資料係從公務機關內部系統性流出的質疑聲浪。因此公務機關平時處理有關民眾資料時，應更加謹慎，以防資料洩漏而影響民眾權益或影響機關聲譽。 3、洩密謀取不法利益： 警務人員每天面對人員之複雜，若無法把持並拒絕錢

		財、女色、酗酒、賭博等各式誘惑，易生價值觀念偏差，常基於不法動機與目的或受業者請託，利用職權謀取私利，不當查詢並洩漏民眾個人資料，行為除涉犯刑法洩密罪及個資法刑事責任之外，若係出自於不正利益的對價交換，更可能觸犯瀆職等重罪。
防治措施		1、提升警務人員個資保密意識： 警察機關洩漏個資事件時有所聞，警務人員為防止危害及預防與偵查犯罪，得依警察職權行使法規定蒐集與利用個人資料，惟應加強宣導警職法第17條「應於法令職掌之必要範圍內為之，並須與蒐集之特定目的相符」規定，以免假借職務不當洩漏或提供他人為不合目的性使用，傳遞警察不當作為將對個人隱私之保護造成極大威脅的觀念，強化警務人員自我約束。 2、落實人員工作考核： 警務人員應落實「警察人員與特定對象接觸交往規定」，主管應關懷了解屬員工作狀況及平日交往，對於品行不佳及有違紀傾向之員警應加強督考或調整職務。如發現重大違紀或有涉案情節，應主動積極偵辦，並追究相關人員行政責任，以達嚇阻效果。
參考法令		1、刑法第132條 2、刑法第216條 3、貪污治罪條例第4條

［案例6：公務信箱註冊外部服務遭駭案］

據報載，衛福部○○署人員帳密個資，疑遭駭客入侵竊取的資安事件，經調查局資安工作站立案調查後，檢調懷疑駭客透過歐洲等地IP作為跳板入侵，先在電腦主機植入後門程式，再竊取帳密個資，不排除是歐洲或大陸駭客所為。KPMG數位科技安全服務執行副總謝昀澤表示，經初步分析比對，此事件與「4月20日美國CDC跟NIH帳密外洩到Pastebin平台上的事件」高度相關，應為公務員使用公務帳號，在如電子商務等外部網站註冊，導致大規模帳密外洩。

（參考資料：中時新聞網）

風險評估	1、密碼保護強度不足： 公務機關均會配發一組電子郵件帳號供同仁公務使用，而許多遭竊資的公務信箱都僅採用辦公室的分機號碼或出生年月日等數字來當密碼，甚至沿用原始預設密碼，並未穿插英文大小寫來將密碼複雜化以提升密碼強度，導致駭客可輕易破解電子郵件，容易造成資安破口。 2、多組帳號共用密碼： 現行許多網站服務都需辦理註冊才能進行瀏覽或提供進階服務，若便宜行事將眾多網站帳號與密碼採取相同組合，只要其中一個帳戶被盜取，其他所有帳戶被攻擊的風險也就大大上升，無形中提高資安風險。
防治措施	1、定期更新使用者密碼： 為確保帳號密碼使用安全性，防止他人不當登入，除使用較複雜的密碼之外，定期變更修改密碼亦有助帳號資料安全。但當發現帳號密碼可能外洩或破解時，應立即變換密碼。 2、公務聯繫限於使用公務信箱： 依行政院秘書長106年1月12日院臺護字第1050190287號函示：「為防止公務資料外洩，各機關同仁應使用機關配發之電子信箱收發公務所需資訊，不得使用非公務信箱進行公務郵件收發。」此外，不應逕行轉發公務電子郵件至非公務信箱處理公務，避免由非公務信箱外洩公務資訊。

		3、公務信箱避免處理私人事務： 依行政院人事行政總處規定，公務員於上班時間，不得從事與公務無關之行為。同仁處理私人事務，應以私人信箱帳號為主，切勿使用公務信箱帳號進行外部服務註冊，更嚴禁於外部網站設定與公務帳號相同的密碼，避免外部網站主機一但被入侵，使用者所擁有的公務信箱、公務資料及個人資料等，都將一起曝險。
		1、行政院及所屬各機關資訊安全管理要點 2、資通安全管理法

［案例7：電子郵件洩漏採購評選委員名單案］

○○市政府文化局約僱人員甲為辦理○○採購案成立採購評選委員會，期間以電子郵件詢問外聘評選委員出席該評選會議之意願，竟疏未注意而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。經地檢署偵辦甲涉犯刑法第132條第2項過失洩漏國防以外之秘密罪，予以緩起訴處分，並命向國庫支付新臺幣1萬元。

(參考資料：法務部廉政署103年8月6日新聞稿)

風險評估	1、採購人員欠缺保密意識： 政府採購法旨在維護公共利益及公平合理的採購環境，因此在本法、採購法施行細則及採購人員倫理準則均規定應保密事項，避免採購人員與廠商有職務關係或機會取得不正利益，影響採購程序公正性。本案採購人員未諳政府採購法保密規定，以致疏忽使評選名單提前外洩。 2、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	1、熟習電子郵件操作： 公務人員除了正式公文與電話之外，十分仰賴電子郵件作為相關業務的溝通聯繫管道，因此公務人員應熟習電子郵件操作方式及撰寫電子郵件應注意事項，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。 2、施以採購教育訓練： 貪瀆犯罪不乏以公務員洩漏採購案件之保密資訊作為前端行為(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法紀觀念。

	3、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，此節應列入平時資安稽核或公務機密檢查項目，提醒同仁注意。
參考法令	1、政府採購法第94條 2、採購評選委員會組織準則第6條 3、採購人員倫理準則第7條 4、刑法第132條

［案例8：洩漏內部簽辦公文案］

據報載，106年間行政院人事行政總處上簽給行政院長關於軍公教調薪政策公文，外洩到全國公務人員協會理事長甲手裡，雖非機密公文，但因公文是採機密作業流程用密封袋處理，竟然還外洩，行政院認為事態嚴重，決定查辦公務部門究竟是誰洩密，追究行政責任。行政院發言人乙表示，公文雖非屬機密公文，但屬重大政策，因此公文陳送是採機密作業流程用密封袋處理。這類公文和人事案同，在行政院院核定後即可對外宣布，公文本身固非機密，但將公文原件（含批示）提供非關之人，仍違反公務紀律。

（參考資料：自由時報）

風險評估	1、公務員負絕對保密義務： 公務員服務法第4條規定公務員有絕對保守政府機關機密之義務，依據文書處理手冊第76點規定：「一般保密事項規定如下：(一)各機關員工對於本機關文書，除經允許公開者外，應保守機密，不得洩漏。」，另依據政府資訊公開法第18條第1項規定：「政府資訊屬於下列各款情形之一者，應限制公開或不予提供之：三、政府機關作成意思決定前，內部單位之擬稿或其他準備作業。但對公益有必要者，得公開或提供之。」，公務人員不可未經機關同意擅自洩漏內部文書，俾免衍生洩密刑責或受行政責任追究。 2、內部文書管理鬆散： 公文書未經允許或簽核准，不得擅自外流、隨意散置或出示他人。下班或臨時離開辦公室，應將公文收藏於辦公桌抽屜或公文櫃內並即加鎖。文書經辦流程及保管應採取適當措施，否則易因疏忽未收妥而遭有心人士伺機窺視或翻閱，造成洩密。
防治措	1、宣導保密義務及法律責任： 保密係公務員應盡義務之一，機關應針對同仁進行公務機密教育訓練及宣導，釐清公務員保密義務不限於「機

施	密等級」。如發現他人涉有危害保密之虞者，即應勸告，其有不聽勸告或已發生洩密情事者，應立即向長官或政風人員報告。 2、遵循公文處理流程： 公務人員不得擅將公文交付他人閱覽、抄錄影印或未經核准電遞、傳真者。申請人如有閱覽、抄錄或攝影政府資訊需求，應依政府資訊公開法及「彰化縣政府及所屬機關學校提供政府資訊收費標準」規定辦理。 3、落實機密文書處理作業程序： 機密文書呈核、呈判或送會，應置於密封公文袋內；如暫不封口則應由承辦人員親自持送，並應儘量減少處理人員層級及程序。外封套不得標示足以顯示內容註記。擬稿、繕印打字之廢件或誤繕、誤印之廢紙，應即時銷毀。
參考法令	1、公務員服務法第4條 2、文書處理手冊第76點 3、政府資訊公開法第18條

［案例9：過失洩漏檢舉人身分案］

甲乙分別任職○○縣○○鄉公所財經課長及秘書，明知依違章建築處理辦法第9條規定，對於檢舉違章建築之檢舉人姓名，應注意予以保密竟疏於注意，於將檢舉坐落○○縣○○鄉○○地號土地上建物為違章建築之檢舉人之姓名，貿然登載於○○鄉公所簡便行文表，並寄發予遭檢舉人。案經福建高等法院金門分院刑事判決，認其係犯過失洩密罪，各處拘役30日，如易科罰金，均以300元折算一日，並緩刑2年。

（資料來源：公務員懲戒委員會89年度鑑字第9161號公懲議決書）

風險評估	1、處理檢舉案件屬應保密事項： 公務員應嚴守保密義務，而公務員服務法僅屬概括規定，實際上是否洩密及是否應加處罰，則散見於刑法及其他法律，承辦人應深入瞭解行政領域中關於受理陳情檢舉之相關細節規定。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。 2、洩漏檢舉人身分常見管道： 洩漏檢舉人資料之過失態樣常見於製作公文書時將檢舉人並列於正副本，或於公文附件、會勘記錄、聯繫資料中未適當隱蔽檢舉人姓名、電話或其他足資辨認出檢舉人身分特徵資料，或有不當聯繫檢舉人導致曝光，甚至基於交往情誼及人情世故而故意洩漏。
防治措施	1、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」、彰化縣政府處理上級機關交付列管及人民陳情案件作業要點第6點第6項規定「案件如涉及當事人隱私、名譽、商（營）業上祕密或其他經法律規定事項，有保密之必要者，除依法應予保密外，受理機關應不予公開。」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，避免因身分資料曝光危害檢舉人。 2、實施個案案例宣導：

		機關辦理教育訓練或例行性宣導，以實際案例適時提醒各機關員工關注切身法律問題，以發揮宣導實效，避免發生類似洩漏檢舉人個資，反致面臨刑事、民事、行政責任追究。
參考法令		1、行政院及所屬各機關處理人民陳情案件要點第18點 2、彰化縣政府處理上級機關交付列管及人民陳情案件作業要點第6點 3、行政程序法第170條 4、刑法第132條

［妨礙使用類］

［案例10：遠端連線竊取他人電腦資料案］

甲為○○市○○區○○國民小學之教師，因其懷疑遭同事乙、丙、丁私下非議，趁乙、丙、丁離開辦公室座位之際，安裝Google免費提供之Google Chrome遠端桌面軟體於乙、丙、丁在輔導室所使用之公務電腦內，並登入甲所使用之Google帳號，啟動遠端連線功能及自行設定一組PIN密碼後，甲再以其於校內辦公室所使用公務電腦內所安裝Google Chrome遠端桌面軟體登入同一組Google帳號及PIN密碼後，得以由其所使用之公務電腦遠端連線操作存取乙、丙、丁公務電腦桌面檔案。甲接續以上開方式自乙、丙、丁之公務電腦內複製取得相片檔案、LINE聊天紀錄、常用私人與公務帳號密碼、輔導公務資料等電磁紀錄，並存放在其所使用之公務電腦內。嗣因乙查覺其公務電腦遭人入侵，通報該校資訊組長協助確認並報警處理，因而循線查獲上情。經法院判決甲犯無故取得刪除變更電磁紀錄罪、洩漏電腦秘密罪、無故侵入他人電腦罪等5罪，應執行有期徒刑6月與有期徒刑9月，如易科罰金，以新臺幣1,000元折算1日。
（參考資料：臺灣臺中地方法院106年訴字第3029號刑事判決）

風險評估	1、電腦權限管理鬆散： 辦公電腦存放許多公務資料，不容忽視辦公室內的資安防護，行為人可以相同手法在不同人的電腦安裝遠端連線工具，足見機關內大部分同仁對於個人電腦的管理及保護措施不足，資安風險控管意識不佳。 2、濫用遠端桌面連線工具： 2020年因疫情影響，多數機關採取分流辦公或居家辦公因應，使用遠端桌面連線功能，能夠輕易實現遠端存取電腦、查看檔案或執行程式，達成遠距辦公目的。惟因遠端存取機制近年易遭駭客利用入侵機關資訊環境或成為攻擊跳板，機關如開放使用遠端桌面軟體連線，應注意電腦暴露在網際網路的風險程度。
防治措	1、設定密碼並勤換密碼： 個人電腦最基本的安全防護便是設定一組開機密碼，即可以防堵他人任意啟動電腦，進而防止他人窺探隱私，然而密碼並非設定後即一成不變，應定期更新密碼並避

施	免將密碼張貼於辦公環境隨手可見之處。 2、善用解除螢幕保護程式密碼功能： 如長時間離開座位，應將電腦設定自動啟動螢幕保護程式及解除密碼，或離開座位時隨手將電腦暫時登出或利用鍵盤組合鍵(Win+L或Ctrl+Alt+Del)或實體快捷鍵，進入螢幕鎖定狀態，預防他人使用。 3、慎選遠端連線工具： 除微軟(Microsoft)內建的遠端桌面功能之外，市面上存有相當多軟體亦可提供遠端連線服務(如Chrome遠端桌面、AnyDesk、Teamviewer等軟體)，如有居家辦公需求，因慎選無資安疑慮之連線軟體，並依機關資安規定進行設定(如VPN、防火牆)，無遠距辦公需求時，中止連線服務，以免遭受駭客入侵。
參考法令	1、刑法第318條之1 2、刑法第358條 3、刑法第359條

［案例11：無故輸入他人帳號密碼案］

甲服役於空軍○○指揮部上士空電士，接受乙請託，確認乙自不明人士處收受甲前夫即丙之電子兵資紀錄（含獎懲資料內容）之真實性。甲經由公務機關電腦設備，輸入丙之國軍電子兵資系統帳號及密碼成功登入，並取得丙之國軍電子兵資電磁紀錄，嗣以通訊軟體LINE訊息向乙確認上開丙之電子兵資紀錄為真實，而洩漏此國防以外應秘密之消息。嗣因丙發現乙在社群網站Facebook社團「爆料公社」中，揭露丙人事懲處等資料之情形，爰向憲兵隊提出告訴。經一審判決甲犯公務員假借職務上之機會，故意犯無故取得公務機關電腦之電磁紀錄罪，處有期徒刑6月。上訴二審改判緩刑2年，並應接受法治教育課程5場次。緩刑期間付保護管束。
（參考資料：臺灣屏東地方法院109年度訴字第399號刑事判決、臺灣高等法院高雄分院110年度軍上訴字第1號刑事判決）

風險評估	1、帳號密碼與他人共用： 公務資訊系統並非人人均可以申請使用或擁有相同層級操作權限，如多人共用同一帳號密碼，發生資安問題時將難以釐清究責。此外，將多組網站或資訊系統共用相同帳號密碼，將使帳號更容易受到駭客攻擊而使帳戶資訊外洩。 2、未更改系統預設密碼： 實務上曾發生同事知悉學校電子郵件網域名稱以及配發教職員工個人電子郵件信箱，以及預設密碼，藉此假冒他人名義，寄送檢舉信函營造具名檢舉之假象。倘有心人士掌握系統或使用者名稱，如未更改系統原始密碼，將使未經允許的用戶能夠輕易嘗試登入。
防治措施	1、帳號密碼專責管理： 公務資訊帳號密碼應由個人善盡保管之責，不任意向任何人提供個人帳號及密碼，當發現密碼有可能遭受破解或竊取之可疑跡象時，應立即變更密碼。 2、替換原始密碼並定期變更： 使用者第一次登入資訊系統時，應馬上更改臨時性啟始

	(預設)密碼，並採取具複雜變化之防禦高強度密碼，並宜定期更換密碼。 3、落實管理使用權限 退(離、休)職人員之帳號密碼應立即取消使用管理權限，並列入退(離、休)職手續中，或通知資訊管理單位更新使用權限。
參考法令	1、刑法第132條 2、刑法第358條 3、刑法第359條 4、刑法第361條

［案例12：無故刪除監視系統畫面紀錄案］

甲在○○市政府○○局服替代役，負責輪值更新主機房內之電子看板管理系統等工作，並因此持有主機房鑰匙。因○○局秘書室職員發覺○○局所購置之宣導用酒數量短少，而開始進行調查，甲向資訊人員乙稱願意協助至主機房內觀看、過濾監視錄影畫面，乙因而將該監視器系統之最高權限密碼「888888」告知甲。詎料甲基於無故變更公務機關電腦之電磁紀錄之犯意，進入主機房內後，輸入監視器系統密碼，進入監視器系統主機，無故以格式化方式刪除硬碟內所儲存之所有監視器畫面電磁紀錄，致無法調閱監視器畫面，足生損害於○○局。第一審依無故變更公務機關電腦之電磁紀錄罪，處有期徒刑4月，第二審及最高法院均駁回甲上訴，全案定讞。（資料來源：臺灣桃園地方法院107年度訴字第466號刑事判決、臺灣高等法院刑事判決110年度上訴字第271號、最高法院110年度台上字第5425號刑事判決）

風險評估	1、電磁紀錄的定義： 刑法第10條第6項規定「稱電磁紀錄者，謂以電子、磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄。」例如電腦的網頁管理資料、儲存在伺服器的帳號密碼、手機平板內的數位照片或影片檔，都算是電磁紀錄。 2、電磁紀錄能否救援恢復與成罪無關： 因電磁紀錄本身具有可複製性，又不具有損耗性，縱被複製亦不致因此而消失，而依現行之科技設備，若要回復被刪除之電磁紀錄，亦非難事，故解釋上，應認電磁紀錄遭受無故刪除時，即已產生網路電腦使用之社會安全秩序遭受破壞之危險，至於該電磁紀錄事後得否回復，均無礙於「變更」、「刪除」之成立。倘其行為，又已致生損害於公眾或他人，即成立犯罪。
防治措	1、研訂錄影監視系統管理規則： 監視錄影設備所攝錄之影音資料原則上應予保密，嚴禁私自拷貝複製或任意公開散布，因此有關查核、檢視、調閱及複製等事項之權限，應遵守行政程序法、政府資

施		訊公開法及個人資料保護法等相關法令規定，並研擬標準作業流程以供遵循。 2、落實專責管理人員： 監視系統機房應採門禁管理，不對外開放，並應指定專人專責操作及管理，如因具體事由需調閱監視系統畫面內容，申請並經機關首長同意後，交由專責人員查看、複製或派員陪同調閱。
參考法令		1、刑法第359條 2、刑法第361條

［案例13：無故竊錄通訊軟體談話內容案］

甲與乙同為臺灣○○地方法院法官，緣甲曾介紹友人丙與乙認識，然不知丙與乙於相識後進而交往一事，之後趁乙因午休外出及不在辦公室之際，進入乙之OA辦公區域，利用乙電腦雖有啟動螢幕保護程式，但為未設定密碼之待機狀態，未經同意解除螢幕保護程式後，無故檢視乙之通訊軟體LINE之好友名單及對話紀錄，並於瀏覽乙與丙談話內容後，認為乙、丙均為各自有配偶之人，遂以行動電話拍攝乙與丙間之親密照片，並告知院長乙涉婚外情。後經乙察覺提起告訴，經第一審判決甲犯竊錄他人非公開活動、談話及身體隱私部位罪，處有期徒刑4月；又犯竊錄他人非公開談話罪，處有期徒刑3月。應執行有期徒刑5月，如易科罰金，以新臺幣1,000元折算1日。沒收部分併執行之。

（資料來源：臺灣桃園地方法院109年度矚易字第3號刑事判決）

風險評估	1、無故行為的定義： 「無故」，係指欠缺法律上正當理由者而言，縱一般人有伸張或保護自己或他人法律上權利之主觀上原因，亦應考量法律規範之目的，兼衡侵害手段與法益保障間之適當性、必要性及比例原則，避免流於恣意。 2、非公開活動的定義： 「非公開之活動」，係指活動者主觀上具有隱密進行其活動而不欲公開之期待或意願（即主觀之隱密性期待），且在客觀上已利用相當環境或採取適當設備，足資確保其活動之隱密性者（即客觀之隱密性環境）而言。
防治措施	1、善用解除螢幕保護程式密碼功能： 如長時間離開座位，應將電腦設定自動啟動螢幕保護程式及解除密碼，或離開座位時隨手將電腦暫時登出或利用鍵盤組合鍵(Win+L或Ctrl+Alt+Del)或實體快捷鍵，進入螢幕鎖定狀態，預防他人使用。 2、慎用通訊軟體傳遞訊息： 機敏資料使用網際網路、電子郵件或通訊軟體傳遞，任一環節都可能遭刺探、蒐集，尤其目前普遍使用即時通

		訊軟體進行溝通(例如Line、Instagram、Telegram、Messenger等)，雖可提升公務聯繫效率，但亦易因疏忽而洩漏相關資訊，且事後追查不易，因此機敏性資料不宜使用通訊軟體傳遞。此外前開通訊軟體伺服器設立於國外，亦有資安外洩的疑慮。 3、不使用資通疑慮之產品 居家辦公或遠距辦公除使用即時通訊軟體聯繫公務之外，常有召開視訊會議之需求，如會議內容涉及機敏性資料，應選擇無資安疑慮之產品，例如zoom曾被揭露多種全性漏洞與隱憂，在利用視訊軟體或服務時皆應更為謹慎。
參考法令		刑法第315條1

［案例14：駭客潛伏攻擊機關資訊系統案］

據報載，「司法駭客」攻擊我國司法院與所屬法院全部29個司法機關，司法院主機遭植入數個惡意後門病毒後，駭客可從遠端存取司法人員帳號密碼，直到台北地院遭到大規模攻擊，全案始爆發。至於判決書是否遭竄改，司法院昨表示未查出類似情形，已將相關事證送行政院資安會報，並擬聯合調查局等追查駭客犯行。一名資深法官表示，現今判決仍以紙本為主，宣判後才會把電子檔上傳司法院系統，就算網路上的判決遭竄改，仍不影響實體判決內容與結果；不過另有法官說，一審法官月審6、70案，如判決書在宣判前遭竄改，印出前又無暇檢視，就有可能出現錯誤裁判。該病毒為零時差電腦病毒，是全新後門程式，資訊處表示，受感染電腦數243台，9成電腦的作業系統為XP，未來將全面更新作業系統，另一是全改為單機，避免中毒；司法院主機也將佈建APT防衛系統，可儘早偵測電腦遭入侵情形。

（資料來源：自由時報）

風險評估	1、電腦作業系統老舊： 微軟已於2021年10月正式發布最新的Win11作業系統，雖然大部分公務電腦均以更新至Win10系統，但仍有部分公務使用的系統平台受限於軟體開發限制，仍運行老舊的Win7或WinXP。如同微軟已停止支援Internet Explorer（IE）瀏覽器安全性更新，但公家機關也有部分軟體限制使用IE的情況，老舊的作業平台與軟體失去安全性更新後，安全性均容易產生隱憂。 2、使用者電腦使用習慣不佳： 安裝來歷不明的程式、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行為，均可能對機關資安的維護造成漏洞。 3、個資法損害賠償採無過失主義： 我國民法損害賠償責任係採過失責任為原則，無過失責任則規範於特別法之中，而依個資法第28條規定公務機關違反本法規定，負損害賠償責任，僅限於天災、事變或其他不可抗力所致者，免負賠償責任。因此當個資是

		從機關外洩，導致侵害個資主體權利的情況下，公務機關負擔的是無過失的事變責任。
防治措施		1、隨時保持系統更新： 惡意軟體往往都是針對系統漏洞進行攻擊，不論使用Windows或Mac系統，都建議按時配合軟體更新，修補漏洞，保持系統為最新狀態，勿自行關閉系統自動更新程式，以免駭客依循系統漏洞入侵系統。 2、開啟防火牆安裝防毒軟體： 防火牆是網路資安的第一道防線，因此內建防火牆必需開啟，才能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，下載使用網路文件檔案，應先進行掃毒，勿任意開啟。 3、重視資料備份的重要性 防毒軟體、設定密碼與更新軟體是安全防護的基本功，但無法百分之百防範外來的攻擊，因此日常進行資料備份係預防惡意軟體或勒索病毒的最佳手段，即使電腦遭入侵資料被感染或上鎖，透過資料備份還原的方式，也能確保重要資料的恢復。
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

［案例15：通訊軟體遭駭客入侵案］

據報載，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。由於這次事件涉及府院高層人士，恐對國安造成重大威脅，國安單位已經展開深入調查，近期遭揭發的間諜軟體「飛馬」（Pegasus）被列入，甚至不排除是否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。

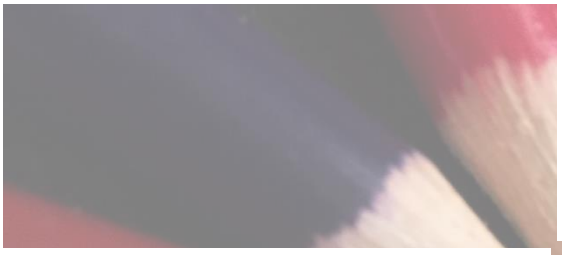
（資料來源：科技新報網路新聞）

風險評估	1、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，資安風險意識之建立不易，忽略駭客會利用惡意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。 2、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有所提升，但社群軟體及通訊軟體早已滲透個人生活之中，企業在使用者未意識到的情況下不斷蒐集個人資料數據及資料分析技術，引起侵犯隱私權的疑慮，使用者勢必在安全、隱私及便利性之間有所取捨。
防治	1、不安裝不明手機軟體： 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

措施	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。 2、不使用不明之公共(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不明免費的公共熱點。 3、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。 4、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貼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

［結語］

資安防護沒有人是局外人，資訊安全攸關機關政策推動及民眾權益之保障，資訊外洩小則侵害個人隱私、大到影響國家安全，而公務員依法負有保密義務，一旦疏怠洩漏，將背負行政責任議處及民、刑事責任。



本府編撰資訊安全防貪指引提供同仁參考，希藉此提升同仁對於資安意識的關注，並以落實縣長政見「建立廉能政府：不濫用行政資源、不公器私用、依法行政、提高行政效率與行動力」之施政理念。