

# 臺中市東勢區公所115年3月份公務機密維護宣導 專欄

## 如何維護資訊安全

如何確保資訊安全與保密工作的完整性，已經成為國家與產業推動資訊化的首要目標，資訊保密實為廉價的資訊安全防護措施，個人對資訊保密工作之認知與重視，可使國家與社會在最經濟之原則下，防杜敵國或產業竊取重要資訊。其次，個人應存有「時時保密」、「處處保密」及「維護機密安全是個人的專業責任」之觀念，尤以當前資訊設備精進，傳遞資訊的速度極快，洩密者或竊密者只要利用資訊設備，即可將所竊取之資訊即時傳遞，進而影響國家安全與競爭力。所以，我們應對週遭異常的人、事、物保持高度之警覺，及增設資訊安全防護設施，例如：設定使用帳號與權限、定期更換密碼、資訊加密、數位簽章等，以避免非相關人員接觸或使用資訊設施或資料，增加洩密之機會。管制作為：

(一) 人員管理及資訊安全教育訓練：各單位於籌設電腦作業系統或辦理委外廠商簽約維護電腦設施時，應依規定完成相關作業及維護人員之安全調查，並於工作執行階段，予以全程監督及必要之保密安全輔導與檢查；另與維修廠商應簽立「保密切結」俾能約束廠商保密之法律責任。擔任電腦作業人員，尤其是系統管理人員，應具備絕對忠於職責、有高度保密警覺、品德端正生活正常、能履行有關安全規定之必要條件，派任工作前，應施以保密安全教育，了解個人保密安全責任，熟悉有關安全要求與方法，對不按規定或屢犯過失者，應適時調整職務，並在決定或提出建議之同時，採取隔離措施。

(二) 落實檢查管制措施：為有效稽核各單位電腦作業情形，發現潛存危因，各級應對所屬電腦系統實施定期與不定期方式之抽檢，並嚴格針對內部成員於作業時之磁片暨檔案

管理情形、密碼設定、傳真機、影印機等設備實施全面性檢查，確保單位資訊作業安全。

(三) 續密資料處理儲存：電腦資料處理應設定安全防護措施，建立稽核制度與預警功能，另個人電腦因其安全防護措施功能較差，應嚴格要求設定開機密碼，在系統未採取任何安全保密措施前，任何分類保密，禁止存放於個人電腦硬碟中。

〔四〕嚴防不法破壞盜拷：視系統所擔負各項任務之機密性、重要性與價值性，設置具自動稽核及違常狀 示警與處理功能之安全防護機制，並將使用者姓名、異動檔案、進入及離開時間等，隨時自動紀錄，定期 出，密交使用單位主管核對，以防資料盜拷。

## 近期案例宣導

### 違法查詢資料洩漏機密遭判刑

壹、案情概述：

一、甲、乙、丙等人分別為稅捐單位之稅務員，為依據法令從事公務之人員，緣起於該等有共同友人丁以徵信社為業，自八十三年間起，丁均以傳真或電話方式通知，用被查詢人身分證字號等資料，請甲等代查個人財產資料，再由甲等利用職務上操作電腦終端機之機會，或利用同事離開座位未關電腦之際，將建檔儲存於電腦中之待查對象個人財產資料，以身分證字號叫出後，再將資料交付或傳真回覆予丁，丁每月委查數十件不等，每件支付甲等人報酬新臺幣二百元不等，丁則將查得資料轉交委託調整之客戶，並收費牟利。

二、本案經地檢署指揮偵辦，偵查終結以甲、乙、丙與丁係共犯貪污治罪條例第六條第一項第四款對於主管之事務直接圖利罪及刑法第一百三十二條第一項洩漏國防以外之秘密罪嫌，依共同正犯提起公訴。本案經臺灣高等法院臺中分院更一審判決，丁處有期徒刑一年三月，甲、乙、丙共同連續對於主管之事務，直接圖利及對於非主管或監督之事務，利用職權機會圖利，均各處有期徒刑二年六月，遞奪公權兩

年；甲、乙、丙之所得財物並予追繳沒收。

貳、研析：

一、甲、乙、丙等人係依據法令從事公務之人員，明知個人財產資料係屬國防以外之機密，非因機關公務所需，不得任內調取，竟利用職務之便提供相關業者牟利，除嚴重影響公務人員形象外，更誤導民眾以為只要有管線即可取得機密資料。

二、少數公務員法令觀念薄弱，保密警覺不足，致同事可任意使用他人電腦，或取得開機密碼，使密封喪失應有之防護作用。

參、檢討分析：

戶政、地政或其他類如警察、稅捐、電信等機關人員係依據業務職掌經管公務機密資料，理應恪遵作業規定，予以保密，不得洩漏於外，即或在人情困擾下，亦不得破例，否則民眾權益及個人隱私勢將受損，坊間多有徵信業者從事錄音、跟蹤、查址、尋人等業務，平時為包攬生意，打探隱私，勢必透過種種方式或管道向公務經管單位取得相關資料，文中某甲將查詢代號洩漏予乙，雖屬基於私人之情誼，亦已觸犯相關法條，如係期約收賄，則必獲從重量刑，上開案例足堪身為公務員者戒。

**「多一分保密警覺，少一分洩密的風險」，每個人都要有此共識與認知，處處小心為要，如此在日常生活及公務處理上，才能建構一個安全的環境。**



**臺中市東勢區公所政風室提醒您**

