

目 錄

一、**廉政小叮嚀：反貪反腐高效率，廉政提昇競爭力。**

二、**洗錢防治宣導—什麼是疑似洗錢申報？**

洗錢防制法第 10 條規定，金融機構及指定之非金融事業或人員對疑似洗錢犯罪之交易，應向法務部調查局申報。(資料來源:行政院洗錢防制辦公室)

三、**廉政宣導**

(一)「圖利與便民」專案法紀宣導：**私運廢棄物，關說犯錯誤**

曾貪心經營一家廢棄物清運公司，如要清運一般事業廢棄物，應向主管機關申請核發廢棄物清除許可文件。但是，曾貪心只想便宜行事，將一般事業廢棄物偷偷運到小島市公所垃圾場隨意傾倒了事，於是找上民意代表賈關懷，請他協助私運事業廢棄物進場。賈關懷與清潔隊隊員放水弟商議後，由放水弟向曾貪心收取每車次新臺幣(下同)1萬8,000元後，即同意進場傾倒，並由賈關懷出面向垃圾場場長倪大偉關說放行事宜，倪大偉害怕賈關懷民意代表的身份，不得已就接受關說。曾貪心私運事業廢棄物到垃圾場時，放水弟就關閉監視器及開啟大門，直接讓車輛進場，每車次所得金額自行取走放行費用1,000元，其餘全數交給賈關懷，總計放行60車次，曾貪心支付108萬元。另外，倪大偉有時在場，卻不加阻止，甚至偶爾駕駛堆土機，幫忙掩埋事業廢棄物，放水弟事後，也會請倪大偉喝酒，並曾交付2,000元，請倪大偉自行拿去買酒喝。賈關懷、放水弟均明知廢棄物清理法第41條規定，從事廢棄物清除、處理業務者，應向直轄市、縣(市)主管機關或中央主管機關委託的機關申請核發公民營廢棄物清除處理機構許可文件，方可進行，卻縱容曾貪心進場傾倒事業廢棄物，並圖得108萬元不法利益。場長倪大偉雖然是被動配合，僅獲得2,000元的微薄不法利益，仍會構成圖利罪。最後，賈關懷、倪大偉、放水弟等3人，被法院依違反貪污治罪條例第6條第1項第4款之圖利罪，判處2年8個月至5年6個月不等有期徒刑，褫奪公權3年。

(二)反賄選宣導：**i 幸福 檢舉賄選 人人有責**

本(108)年第十屆立法委員暨第十五任正副總統選舉，將於109年1月11日投票。本次選舉反賄選之宣導口號為「i 幸福 檢舉賄選 人人有責」；有關法務部及廉政署製發之反賄選宣導素材(含宣導海報、宣導影片、廣播插播卡等)已上傳至本家全球資訊網「最新消息」及家區內網「公告區」→「政風宣導」→「108年政風宣導」資料夾中，請各組室、各堂及全體同仁撥冗瀏覽，廣為宣導。

四、**保防宣導短片-假消息**

為強化機關安全管理防衛機制，提升同仁安全保防意識，已於本家網頁/訊息公告/資訊公開/政府資訊項下，連結法務部調查局「保防宣導短片-假消息」，請各同仁踴躍上網點閱觀看。

五、**公務機密維護宣導—現代生活應具備的保密觀念**

身處在這個資訊交遞快速的 e 時代裡，現代人均普遍利用各類事務機器及通信、資訊設備，俾能快速連絡及處理各類事務，然此同時，您是否已確實做好相關保密措施，來確保機密資料不外洩呢？茲提供左列事項參考，期能建立保密共識：

文書作業應注意保密事項

一、重要應秘密事項避免書寫於便條紙或桌曆上，以防遭人窺視或翻閱，造成洩密。二、具機密性之廢棄文稿應隨手銷燬，以免遭人蒐集重整復原，切勿逕交清潔工清運，以免機密資料外流；影印重要文件如遇夾紙應即取出，印壞部分亦須銷燬，以免被有心人取走做不當利用。三、傳真機密文件前，應先連絡好收件人於傳真機旁等候，傳送前須先確認傳送號碼無誤、傳送完成前不可離開，以免遭人窺視或取走而致洩密。

資訊作業應注意保密事項

一、個人電腦單機作業或辦公室區域網路連線，須設定密碼保護，並定期變更密碼；螢幕保護裝置亦應設定密碼，以防暫時離座時遭人窺探畫面內容。二、內部網路做檔案資源分享時，應妥慎審核資訊內容是否涉及機密事務，如涉及機密事務應避免為分享之資源。

三、各種經常使用之密碼，如 E | Mail 帳號、網頁設計密碼等，切勿以另紙書寫置於電腦或辦公桌明顯處，且禁用各種作業系統內建之「自動記憶密碼」功能，否則將喪失密碼保護功能。

四、勿任意上網登錄個人重要應秘密資料，以免遭截或竊取移作其他不當用途。（資料來源：臺北榮民總醫院政風室）

六、**機關安全維護宣導—小心檔案被竊**

法務部調查局發現，有歹徒利用電子郵件 PDF 檔夾帶惡意攻擊程式，自動聯結特定網站下載木馬程式，竊取被害電腦中的檔案、照片等資料，提醒民眾注意防範。近期，調查局陸續接獲主旨「調查局沿革職掌」，附加檔案「調查局沿革職掌.PDF」的電子郵件，發現該 PDF 文件，是利用 Adobe Reader、Acrobat 軟體 8.1.1 以前版本的漏洞，點選後會聯結特定網站下載木馬程式到電腦系統中，進而竊取資料。歹徒竊取的資料包括網路銀行、線上購物、個人信箱的帳號密碼、電腦系統中之文件與照片，以及鍵盤側錄、隨身碟內的檔案資料等。調查局分析，此一攻擊模式，是利用處理 PDF 的 Adobe Reader、Acrobat 軟體，在 JavaScript 處理流程中，會產生緩衝區的

漏洞，攻擊者利用上述漏洞執行任意程式碼。犯罪集團利用各種吸引人的電子郵件標題與內容，誘使收件者點選打開郵件附加檔案。由於PDF檔案格式已是全世界主流文件格式，民眾應特別注意。

調查局籲請電腦使用者可依下列程序，防止中毒或減少受損程度。一、儘速下載Adobe Reader、Acrobat軟體更新檔案至8.1.2版，避免類似攻擊情況持續擴大。二、在微軟IE瀏覽器關閉自動開啟PDF文件功能，並設定IE在開啟PDF檔案時先提醒，將「瀏覽器中顯示PDF (Display PDF in browser)」，變更Windows registry設定。

(資料來源:臺北榮民總醫院政風室)

臺北榮家政風檢舉專線電話(外線：02-26732618，內線：904)

臺北榮家政風檢舉電子郵件信箱：yhtpe0015@mail5.vac.gov.tw

(廉政檢舉專線: 0800-286-586、傳真: 02-2381-1234)