



農業部動植物防疫檢疫署

2024 6月號

廉政暨維護電子報

目錄

- 廉政案例
- 履約管理(含契約變更)廉政宣導
- 資訊安全
- 消費者保護

1

法務部廉政署南部地區調查組偵辦高雄市政府交通局車輛行車事故鑑定委員會主任委員許○○違反貪污治罪條例等案件，業經臺灣高雄地方檢察署檢察官偵結提起公訴。

許○○自民國106年8月15日起至112年1月13日止，擔任高雄市政府交通局車輛行車事故鑑定委員會（下稱車鑑會）主任委員，對外代表該委員會，對內負責行車事故鑑定等業務，並綜理監督該委員會之行政事務。詎許○○明知車鑑會之機關首長特別費之報支，須以「各級政府機關特別費支用規定」說明一之（一）所規定之使用範圍為限，竟利用核銷特別費之承辦人員均尊重其首長職務、信任其報支之消費均符合上開規定使用範圍之慣例，及利用核銷特別費之承辦人員並無實質審查權之漏洞，持其家人或私人朋友用餐等不符合特別費報支範圍之發票核銷特別費，總計詐得新臺幣1萬 1,639元。

案係本署南部地區調查組與臺灣高雄地方檢察署共同偵辦，並協請內政部警政署保安警察第五總隊參與協助，經執行搜索及約詢相關人到案，許○○對於上開犯行坦承不諱，並已主動繳回全部犯罪所得。嗣檢察官偵查終結，認許○○涉犯貪污治罪條例第5條第1項第2款之利用職務機會詐取財物罪嫌、刑法第216 條及第214條行使公務員登載不實公文書等罪嫌，予以提起公訴。

資料來源：法務部廉政署113年6月3日發布



2

履約管理(含契約變更)廉政宣導

案例4-【收受賄賂讓業者簡化採購項目規格履約】

【事實】

大秉擔任某榮譽國民服務處輔導員，接受廠商「放水就給好處」的邀約，明知廠商於辦理單身亡故榮民公祭時，提供之樂隊或抬棺工人人數不符合契約規定，卻仍在驗收紀錄上登載「與契約相符」字樣，並於機關核銷付款後收受廠商的賄款或香菸。此外，尚有幾場公祭，廠商雖依契約規定履約，大秉仍收受廠商提供的賄款或香菸。



2

履約管理(含契約變更)廉政宣導

【補充】

同仁於廠商提出賄賂邀約時，即應拒絕並通報長官、政風室或輔導室等相關單位。因為同意賄賂邀約，即涉犯期約賄賂等罪，而廠商是否依契約規定履約，僅係「違背職務」或「不違背職務」賄賂罪之法條適用差異。

本案中，大秉在廠商依契約規定履約之幾場公祭後收受賄款或香菸，即被法官認定為「廠商希望大秉通融、好過」之不法對價關係，大秉仍觸犯貪污治罪條例不違背職務收受賄賂罪。

【相關法條】

貪污治罪條例第4條第1項第5款之違背職務收受賄賂罪及刑法第216條、第213條之行使公務員登載不實文書罪；貪污治罪條例第5條第1項第3款不違背職務收受賄賂罪。

資料來源：農業部113年履約管理(含契約變更)廉政宣導案例彙編

3

常見5大資訊安全威脅與對應資安防護措施

1.網路安全：

是指針對連接網路裝置、網路中傳輸的資訊、利用網路運作的軟體及透過的服務，這些項目的安全都包含在網路安全範圍內，有心人士會透過對網路的侵害，來達到竊取敏感資訊，癱瘓裝置、軟體或服務等，進而製造出個人的身份被盜用與詐騙，甚至是企業的重要資料被竊取或無法正常營運等問題。

★合適的資訊安全措施：面對DDoS攻擊的主動式DDoS緩解服務、MDR威脅偵測應變服務、網管監控服務、資安顧問諮詢、資安防護架構規劃。

2.系統安全

電腦系統或者網站系統的安全，會隨著技術的日新月異，隱藏於其中的缺陷也隨之浮現或被發掘，這些缺陷我們通常稱之為漏洞，而漏洞的存在將使得系統和資料的保密性、完整性、可用性、授權機制都面臨有心人士的威脅。針對系統安全，通常會透過對漏洞進行管理作為應對措施。漏洞管理的第一步就是定期進行資安檢測，如系統弱點掃描，並以風險為依據排定補救措施優先順序。此外最好隨時檢測資訊環境中是否存在異常的網路行為，以提前發現漏洞。

3

常見5大資訊安全威脅與對應資安防護措施

★合適的資訊安全措施：定期資安檢測(網站弱掃、系統弱掃)、MDR威脅偵測應變服務、網管監控服務、資安顧問諮詢、資安防護架構規劃。

3.應用程式安全

上述說明中有提到軟體安全中包含了應用程式安全，而應用程式玲瑯滿目，更與生活也息息相關，從文書作業、訊息的傳遞到商業的交易都有應用程式的存在。我們需要了解如何避免有心人士從應用程式的運作中，找出潛藏的漏洞，進而用以侵害個人隱私，財產甚至是人身安全。因此使用者必須留意且重視正在使用的應用程式之來源、發佈應用程式的單位或組織是否主動地檢視程式的安全性，並在整個應用程式生命週期內保護程式避免威脅迫害。降低網路犯罪者找出並利用應用程式中的漏洞來竊取資料、智慧財產以及機密資訊等行為。

★合適的資訊安全措施：定期資安檢測(網站弱掃、原始碼檢測、App認證)、資安顧問諮詢、資安防護架構規劃。

常見5大資訊安全威脅與對應資安防護措施

4.資料加密及身份認證授權

在資料安全上除了確保資料的保存外，也要考慮到資料被竊取的可能性，目前有許多的機制及技術能對資料進行加密，讓非經授權的有心人士無法識別及解讀，萬一發生被竊取時，可以藉此增加對資料的保護能力，降低損害。近期頻傳的勒索病毒也是對資料保護的嚴重考驗，過去單純保護資料不被竊取的方式，已經無法滿足這種惡意行為，必須採取新的資安思維及防護技術來保障資料。現今的生活中，已不再需要到特定地點辦理，使用網路就可以執行，大大地增加便利性，但隨之而來的問題是如何確保身份認證的授權身份、資料的管理及使用。近年來國際間提出許多相應的規範與認證，政府單位、金融機構服務及企業網站，可以參考或遵循國際標準或國家規範，來保護及使用民眾的資料。

★合適的資訊安全措施：防勒索雲端儲存服務、資安憑證(SSL憑證)、資安顧問諮詢。

常見5大資訊安全威脅與對應資安防護措施

5.雲端安全(雲端運算安全)

所謂的「雲端運算」與傳統電腦系統及架構不同之處，雲端運算是一定要透過網際網路來使用可共享的軟、硬體資源之運算技術。由於雲端運算是依靠著網路來實現，並且能將架構中的軟、硬體及應用程式，以共享的方式提供給不同用戶使用，因此在討論雲端運算安全時，必須將網路安全、系統安全、應用程式安全及資料加密安全及身份認證授權等條件一起考量，所以一個可靠且值得信賴的雲端運算環境必須同時具備多個面向的安全能力。

★合適的資訊安全措施：專業可靠的公有雲服務、自建雲服務、混合雲服務

資料來源：數位通國際網站

4

出國旅遊切勿攜帶肉製品回國，以免受罰

財政部關務署表示，暑假一向是國人出國旅遊旺季，尤其近2年入出境旅客人數持續增加，海關查獲旅客違規攜帶豬肉製品案件亦大幅上升，籲請民眾暑假旅遊回國時，務必注意相關規定，切勿攜帶肉製品回國，以免受罰。

關務署進一步說明，海關持續與農業部動植物防疫檢疫署（下稱防檢署）等邊境查緝機關合作，加強查緝來自非洲豬瘟高風險地區入境旅客行李、郵包及進口快遞貨物。自113年1月至5月，海關查獲未經檢疫豬肉及豬肉製品473件349.9公斤，其中以旅客行李查獲313件224.7公斤最多，占整體緝獲件數達66.2%，重量達64.2%，顯示旅客違規攜帶肉製品風險仍高。

資料來源：行政院消費者保護會網站

4

出國旅遊切勿攜帶肉製品回國，以免受罰

關務署為防止含非洲豬瘟病毒肉製品藉由旅客攜帶進入國內，持續與防檢署加強邊境查緝，對來自疫區入境旅客手提及託運行李實施100% X光檢查，請民眾勿心存僥倖，也請告知境外親友切勿攜帶或寄贈豬肉製品，一旦查獲，均移由防檢署依法裁罰，以攜帶來自非洲豬瘟疫區豬肉及其製品為例，初次查獲即處新臺幣20萬元罰鍰，外籍人士如未繳清罰鍰，即拒絕其入境。請民眾勿以身試法，大家攜手努力，共同防堵非洲豬瘟等動物傳染病入侵，維護我國農畜產業永續發展及國際聲譽。



資料來源：行政院消費者保護會網站

廉能是政府的核心價值

貪腐足以摧毀政府形象

公務員應堅持廉潔 拒絕貪腐



廉政檢舉專線 0800-286-586