



法務部矯正署所屬矯正機關 111 年 「公務機密維護」宣導參考教材

案例 1：公文便宜行事，回覆陳情人副知被陳情機關案

一、案情概述

101 年 5 月間，民眾陳情某機關職員 B 延長病假未符規定，案經甲機關收文辦理，惟甲機關承辦人 A 於查明本案始末後，於回覆陳情人同時，副本知會被陳情人 B 所任職之機關，進而暴露陳情人身分。

二、涉及法規：

- (一) 行政程序法第 170 條。
- (二) 行政院及所屬各機關處理人民陳情案件要點第 18 點。
- (三) 法務部矯正署處理人民陳情案件作業要點第 11 點。

三、原因分析：承辦人疏未注意具名陳情人之保密必要性。

承辦人 A 於承辦案件時副知陳情人 B 所任職之機關係一般公文承辦之程序，惟依照行政院及所屬各機關處理人民陳情案件要點第 18 點及法務部矯正署處理人民陳情案件作業要點第 11 點：人民陳情案件有保密之必要者，受理機關應予保密(處理時應予保密)。」本案係陳情公務機關職員之差假問題事項，案屬「行政違失之舉發」，為保護舉發行為之揭弊者免受揭弊之舉而受侵擾，難謂無保密之必要性，承辦人 A 疏未注意具名陳情人之保密必要性，而未進行相關保密措施。

四、興革建議：

- (一) 回覆民眾陳情案件之保密措施改善。

機關於回覆民眾陳情案件時，應雙稿或分旨分文方式辦理，並於函覆時隱匿足資辨識陳情人之資訊，各級主管於公文核稿時亦應落實文書保密規定，以確保陳情人身分不致外洩。

- (二) 人民陳情案件不論機密與否一律隱密陳情人資訊。人民陳情案件若經檢視非列為一般公務機密文書，仍應於辦理時採取適當保護措施，如將載有足以辨識陳情人之資訊隱去，避免有洩漏陳情人身分疑慮。



法務部矯正署所屬矯正機關 111 年

「公務機密維護」宣導參考教材

案例 2：機敏性資料使用後未予銷毀致外洩案

一、案情概述：

某機關同仁 A 為參與機關聯席會議，於會前列印會議中相關高關懷名單，但會中未使用，回辦公室後一時疏忽忘了將名單銷毀，直接丟入廢紙回收箱，嗣後被不知情同事 B 拿給名單所列身分對象 C 再利用，導致部分名單當事人看到名單內容，B 發現後連忙回收，但已被名單當事人 D 用手機拍下外傳，全案經考績會決議核予 A 申誡 1 次處分。

二、涉及法規：

- (一)個人資料保護法第 2 條。
- (二)個人資料保護法第 16 條。
- (三)個人資料保護法第 28 條。
- (四)個人資料保護法第 41 條。

三、原因分析：持有機敏性資料者，未善盡保管責任。

依據個人資料保護法第 28 條「公務機關違反本法規定，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。」之意旨，公務機關之同仁因處理公務而持有機敏性資料者，應本於職責避免該資料遭不法蒐集、處理、利用或其他侵害當事人權利(下稱，資料遭不法情事)，負有保管責任，惟本案 A 疏未將機敏性資料銷毀而直接丟入廢紙回收箱，導致機敏性資料外流，未善盡相關保管責任。

四、興革建議：

(一)加強機敏性資料之使用管理。

機敏性資料應避免列印，若有列印需求得加註「個人資料」、「密」等字樣，以提高承辦人警覺心。

(二)會議使用機敏性資料，應善盡保密措施及相關宣導。

機敏性資料於開會前應提醒在場人員遵守相關保密規定，並可將資料編號請在場人員簽收領取，會後若無保有必要，承辦人應行回收銷毀。

(三)未列密件但涉及個人隱私或個人資料，應確實維護管理資料之運用，除使用上需注意係執行法定職務必要範圍內，並與蒐集之特定目的相符，更應注意列有個資紙張不得作為回收使用，並於使用後確實銷毀，以防個人隱私或個人資料外洩之可能性。



法務部矯正署所屬矯正機關 111 年 「公務機密維護」宣導參考教材

案例 3：視同作業收容人窺視密碼不當使用公務電腦案

一、案情概述

某監所合作社視同作業人員利用平日主管開啓電腦輸入密碼時窺視並記下密碼，再趁主管外出送貨及盤點合作社庫房每日香菸與電池庫存之空檔時間，輸入密碼進入主管電腦調閱其他收容人個人資料。

二、原因分析

(一) 值勤管理員警覺性不足

管理員業務繁忙，作息及暫離時間易遭視同作業收容人掌握，如又未確實離開座位即設定螢幕保護程式及定期更改密碼，易致視同作業人員伺機使用公務電腦調取資料或其他違規行為。

(二) 未定期更改電腦登入密碼或自然人憑證的密碼

管理員於輸入密碼時，疏於防範遭視同作業人員窺探並記憶密碼，或未使用自然人憑證進行系統登入，並於離開座位時將自然人憑證隨身攜帶，致視同作業人員

三、興革建議

(一) 加強公務機密宣導以及教育訓練

各機關利用主管會報及合作社會員宣導現行法令規定、資訊安全措施、相關洩密案例以及可能導致洩密管道等方式加強宣導，務使每位同仁均能了解相關保密規定、法律責任及具體作為，以養成落實資訊安全之使

用習慣，強化同仁戒護勤務之警戒心及危機感。

(二)落實資訊安全稽核

機關應定期或不定期稽核同仁電腦是否設開機密碼、螢幕保護程式及每半年更新密碼，並加強宣導個場舍主管於使用電腦輸入個人密碼時，應避免視同作業收容人窺視密碼，若使用自然人憑證離座時要隨身攜帶，以防憑證遭不當使用。

(三)強化主管考核監督

主管獲知屬員業務涉及公務機敏資料時，除應善盡督導之責任外，若屬員有工作不力、交往複雜、財務狀況不良、經濟來源可疑，或曾遭檢舉操守風評不佳時，則應提前加強輔導考核作為，並適採必要之防處作為，以防範洩密情事發生。