○○部違反資通安全規定檢討案例

壹、前言

公文是政府機關推動公務、溝通意見的重要工具，公文本身能否發揮功能，與行政效能有極密切關係。為因應業務發展需要，行政院於 99 年 3 月修正「事務管理手冊」文書處理部分，對於公文製作程式、結構、表達方式、處理程序及流程管理，以及文書自收文或交辦起至發文歸檔止之流程提供相關作業規定，並針對其他現行規定不合時宜之處予以修正，例如修正規定第八點「…，將公文之處理以電子方式在安全之網路作業環境下，採用電子認證、權限控管或其他安全管制措施並在確保電子文件之可認證性下，進行線上傳遞、簽核工作。」。

另依據行政院研考會 99 年 5 月修正「文書及檔案管理電腦化作業規範」第十一點規定，電子檔案管理應達成下列目標：一、真實性（authenticity）：指可鑑別與確保電子檔案產生、蒐集及修改過程之合法性。二、完整性（integrity）：指電子檔案管理過程，應確保儲存電子檔案內容、詮釋資料及儲存結構之完整。三、可及性（accessibility）：指藉由電子檔案保存機制，配合法定保存年限，維持電子檔案及其管理系統可供使用。因此檔案管理不僅是保存國家發展見證的基礎工作，更是落實政府知識管理的活水泉源；檔案管理工作之目的，就近程而言，在於保存各機關各項行政紀錄資料，就長遠觀點來看，則在於維護國家歷史文化資產。

綜上，公文電子檔案管理工作具有提升效能、保存國家發展見證及落實政府知識管理之目的，而其目標則是維持公文之真實性、完整性與可及性。

貳、案情摘要

○○部○○室○○科科員李○○，於 98 年 5 月 4 日發現渠以原

有帳號密碼輸入電腦卻遭拒絕登入，經聯繫資訊單位承辦系統分析師劉○○調閱電腦存取紀錄檔，發現○○司科員劉○○冒用李○○帳號密碼登入該部公文檔案管理系統，並擅自竄改帳號密碼，導致李○○於 98 年 5 月 4 日因電腦強迫更換電腦密碼指令，渠以原有密碼輸入電腦卻遭拒絕登入，遂將上情陳報科長陳○○並請劉○○至該科說明帳號密碼取得管道，惟劉○○卻表示係電腦自動出現多組帳號密碼，渠僅隨意選取使用，非其刻意竊用等語，李○○為防範該部檔案資料因此外洩，爰於 98 年 5 月 5 日將上情通報政風處。案經該處洽請資訊單位初步清查，發現劉○○自 96 年 11 月 19 日起至 98 年 5 月 1 日止，即以個人公務電腦利用○○室○○科科員李○○帳號密碼登入該部公文檔案管理系統瀏覽或列印公文，嗣經初步清查結果總計瀏覽 21 個單位、632 筆（1452 次）資料；瀏覽且列印公文 13 個單位 372 筆，經深入清查結果發現，其中除 6 件涉及獎懲個人資料外，餘均非屬機敏公文。

依據劉○○自白書及訪談相關人員，案情摘述如下：

科長蕭○○於 96 年 11 月間由○○室○○科長調任○○司科長，某日因急於參加會議，適劉○○表示公務急需調閱公文，必須取得蕭○○之調閱檔案權限，因蕭○○到任不久且忘記新核發帳號密碼，遂徵得不知情之前任職○○科同仁李○○同意，將其帳號密碼提供劉○○調閱公文使用，惟蕭○○事後曾於公開場合向劉○○及全科同仁宣示，該帳號密碼非屬該科權限，不得使用…。惟劉○○自 96 年 11 月 19 日起至 98 年 5 月 1 日止，冒用李○○帳號密碼登入該部公文檔案管理系統，時間連續長達 1 年 6 個多月，嗣因檔案系統強制更新帳號密碼，劉○○誤植輸入自己帳號密碼，導致 98 年 5 月 4 日李○○以原有之帳號密碼輸入電腦卻遭拒絕登入，經追查電腦 IP 位址，始知遭劉○○長期冒用。

劉○○行為除已違反「檔案檢調作業要點」第2點「借調檔案以與

承辦業務有關者為限。因業務需要，借調非主管案件時，應送會承辦業務主管同意，或簽請本機關權責長官核准。」之規定，經該部98年○○月○○日考績會第○次會議核定記申誡2次外；亦構成刑法第358條「無故輸入他人帳號密碼、破解使用電腦之保護措或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」、同法第359條「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」及同法第361條「對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。」等犯罪要件。該部政風處爰依規定簽陳部次長核准後，函請檢調機關偵查，並經臺灣台北地方法院審理結果，認定劉○○違反刑法第358條、第359條、第361條罪責，於99年4月9日判處拘役55日，緩刑2年並應於判決確定之日起一年內，向公庫支付新台幣8萬元。

叁、違規發生原因及癥結所在

一、便宜行事提供存取權限帳號密碼

科長蕭○○因渠到任新職且忘記新核發之帳號密碼，在便宜行事考量下，徵得不知情前同仁李○○同意，將其帳號密碼提供劉○○調閱公文使用，雖然事後曾於公開場合向劉○○及全科同仁宣示，該帳號密碼非屬該科權限，不得使用…。惟仍讓劉○○有機可乘，冒用李○○帳號密碼登入本部公文檔案管理系統，瀏覽 21 個單位、632 筆（1452 次）資料；瀏覽且列印公文 13 個單位 372 筆，及變更李○○電磁紀錄等違法行為。

二、未定期更新存取權限帳號密碼

劉○○冒用李○○帳號密碼登入該部公文檔案管理系統，時間連續長達 1 年 6 個多月，嗣因檔案系統強制更新帳號密碼，劉○○誤植輸入自己帳號密碼，導致李○○以原有之帳號密碼輸

入電腦卻遭拒絕登入，經調閱電腦存取紀錄檔，始發現登入之帳號密碼已變更，但登入之電腦 IP 位址卻非其所屬，追查結果始知遭劉○○長期冒用。

肆、改進建議

一、賡續辦理員工資安訓練

該部為提升員工資通安全素樣，每年雖配合行政院資通安全會報工作需求、相關資通安全法令增（修）訂及該部資通安全狀況，委請專家學者定期舉辦 2 次員工資通安全講習，惟仍有少數員工或因公務需要、或因同事之請，基於便宜行事而提供自身帳號密碼，事後卻未將帳號密碼更新，致發生資安違規事件。未來仍應賡續深化辦理員工資通安全訓練內涵，尤應著重於員工自身電腦使用注意事項，以降低違規事件發生。

二、強化個人電腦使用稽核

為防範該部同仁任意下載使用非法或未經授權程式，該部定期委託資訊顧問公司實施個人電腦使用內部稽核，惟考量業務推動及人力因素，僅能以抽籤（單位）及抽樣（人員）方式實施，而產生漏洞。未來應視人力狀況，擴大點、線、面個人電腦使用內部稽核，預先防範該部同仁發生資安違規事件。

三、落實並提升檔案管理功能

檔案管理之良窳攸關本部公文之真實性、完整性與可及性。除應符合行政院研考會 99 年修正之「文書及檔案管理電腦化作業規範」中之作業及技術規範外，使用者更應定期更新帳號密碼及堅守不任意提供他人知悉之工作準則，系統管理者亦應定期檢視使用者記錄檔並設定帳號密碼定期更新功能設定，避免類似資安違規事件發生。

四、增加使用者登入紀錄顯示功能

為防範類似問題再度發生，建議於系統維護及後續系統開發

中，增加「使用者前次登入紀錄顯示」，俾利使用者清楚瞭解上次使用系統時間，防範遭長期盜用問題再度發生。

伍、結語

早期文書檔案工作多屬靜態內部作業，但在檔案法實施及資訊科技潮流之影響下，公文檔案力求標準化、專業化、資訊化及應用價值擴大化，而被賦予動態生命。惟在檔案管理資訊化後，作業流程中若干決策點仍須由人工作業判定，本案由於系統使用者機警，在發現無法登入專屬帳號密碼後，隨即清查並即時通報，始能防止違規事件持續進行，顯示該部平時員工資通安全教育訓練具有一定成效；另在清查過程中，未發現有機敏資料遭瀏覽列印，顯見該部對機敏檔案管理工作十分紮實。在資訊全球化時代，如何有效提昇檔案管理行政效率及積極改革創新，並能有效確保資通安全，實有賴全體同仁共同努力。