統　計　專　題　報　告

高雄市政府政風處暨所屬政風機構
100 年度辦理資訊稽核成效研析

高雄市政府政風處
撰寫人：阮世昌
中華民國 101 年 7 月

目錄

表錄

圖錄

高雄市政府政風處暨所屬政風機構100年度辦理資訊稽核成效研析

壹、前言

我國自民國 87 年開始推動以網際網路為基礎之電子化政府，12 年來已經順利完成第一階段的政府網路基礎建設、第二階段的政府網路應用推廣計畫以及第三階段著重社會關懷、提供民眾無縫隙的優質政府服務。至今無論在提升效率及服務品質方面，已有相當具體的成果，並獲得國際組織評比肯定，顯示電子化政府的成效，已從政府行政簡化、為民服務品質提升逐步擴及政府良善治理、社會公平參與，進而帶動社會及經濟發展等層面，並邁向更具積極意涵之數位機會推動[1]。由此可知，政府電子化之程度足可與世界接軌，惟電子化的普及有其優點，亦存有機敏資料或個人資料外洩之資安事件風險。

承上所述，「資通安全」係政府推動電子化政府一大課題，又「資通安全」包含 2 個含意，分別為「資訊安全」（Information security）與「通訊安全」（Communicationsecurity）。其中「通訊安全」係指確保電子資料在網路傳輸及交換時之安全管控，屬資訊科技專業技術之層面（如電子簽章、防火牆、身份驗證、...等電子管控技術）。另「資訊安全」則係指有關資訊處理、資訊作業及資訊內容之安全。資訊安全威脅可簡分為人為威脅及非人為威脅 2 類。基本上而言，非人為的資訊安全對於組織通常會造成非常嚴重的傷害，雖然威脅產生的機率較小，但是一旦發生，組織如果沒有一定程度之防範，可能造成組織相當大的損失，例如天災（水災、地震）。另一則屬人為威脅，種類則

[1] 資料來源行政院研究考核發展委員會，網址：http://www.rdec.gov.tw/np.asp?ctNode=11967&mp=100。

是相當多元化。威脅來源的產生可分為非組織成員及組織成員2 種，對非組織成員之預防，組織可以透過資訊科技專業技術，阻擋網路駭客非法入侵資訊系統，且可透過各種保全措施，防止非組織成員破壞資訊安全，但對於組織成員，卻無法確保其不會做出危害組織資訊安全之行為。又組織成員對於危害機關資訊安全之行為，傷害遠超越非組織成員所造成的傷害。[2]

根據行政院主計處調查（2008 年統計資料），我國行政組織受資安事故侵害尚難有效控制，如學校近年來受侵害比例居高不下，儼然成為資安防護漏洞的死角（如表格 1）。另近年因資安事故而洩漏資料或資料被破壞之比例有逐年增長的態勢，其中又以學校較為嚴重（如表 2）；又我國組織遭受病毒攻擊比例為 53.2%，比例並不低。比較各組織類別，政府機關（構）控制病毒侵害的能力明顯較高（如表 3），但被感染病毒的電腦，每年仍有上升之趨勢。且遭傀儡程式感染之殭屍電腦可能成為駭客攻擊跳板，甚至導致其他資安事故的發生，可見防範傀儡程式感染議題之重要性，惟學校遭受傀儡程式比例仍為各政府組織類別中最高者（如表 4）[3]。

表格 1 組織遭受資安事故侵害之比例

	97年度遭遇資安事件		96年度遭遇資安事件		95年度遭遇資安事件	
	使用電腦家數	%	使用電腦家數	%	使用電腦家數	%
總計	42,695	54.77	39,874	52.40	32,626	51.85
民營企業	37,861	55.52	35,067	53.07	27,834	52.31
政府行政機關	1,710	39.47	1,675	36.30	1,672	36.30
公營事業機構	407	25.31	399	24.56	404	27.97
公立學校	2,274	55.41	2,287	54.70	2,262	57.25

[2] 吳倩萍，2006，＜政府機關個人資訊安全認知與行為之探討＞，國立臺北大學公共行政暨政策學系碩士論文，4。

[3] 2010 年資通安全白皮書，74-76。

公立研究機構	41	48.78	43	41.86	43	39.53
私立學校	348	76.15	349	77.65	351	78.35
私立研究機構	54	72.22	54	68.52	60	80.00

資料來源：2010年資通安全白皮書。

表格 2 資料遭竊或被破壞之比例表

	97年度 私人資料洩漏		96年度 私人資料洩漏		95年度 私人資料洩漏	
	使用電腦家數	%	使用電腦家數	%	使用電腦家數	%
總計	42,695	2.23	39,874	1.52	32,626	0.80
民營企業	37,861	1.99	35,067	1.50	27,834	0.76
政府行政機關	1,710	3.80	1,675	0.72	1,672	0.48
公營事業機構	407	0.49	399	-	404	-
公立學校	2,274	5.15	2,287	2.49	2,262	1.41
公立研究機構	41	2.44	43	-	43	-
私立學校	348	3.74	349	2.87	351	2.85
私立研究機構	54	1.85	54	2	60	-

資料來源：2010年資通安全白皮書。

表格 3 遭遇病毒侵害之比例

	97年度 電腦病毒攻擊		96年度 電腦病毒攻擊		95年度 電腦病毒攻擊	
	使用電腦家數	%	使用電腦家數	%	使用電腦家數	%
總計	42,695	53.20	39,874	49.48	32,626	49.87
民營企業	37,861	54.51	35,067	50.92	27,834	51.33
政府行政機關	1,710	33.74	1,675	28.36	1,672	28.83
公營事業機構	407	23.83	399	21.55	404	24.01
公立學校	2,274	48.86	2,287	44.43	2,262	48.32
公立研究機構	41	43.90	43	32.56	43	30.23
私立學校	348	67.24	349	70.49	351	71.79
私立研究機構	54	70.37	54	64.81	60	78.33

資料來源：2010年資通安全白皮書。

表格 4 遭遇傀儡程式感染之比例

	97年度 遭遇傀儡程式		96年度 遭遇傀儡程式		95年度 遭遇傀儡程式	
	使用電腦家數	%	使用電腦家數	%	使用電腦家數	%
總計	42,695	10.68	39,874	9.34	32,626	7.05
民營企業	37,861	11.57	35,067	8.91	27,834	5.83
政府行政機關	1,710	0.94	1,675	6.75	1,672	6.46
公營事業機構	407	0.25	399	5.26	404	6.44
公立學校	2,274	3.42	2,287	14.30	2,262	18.30
公立研究機構	41	0.00	43	13.95	43	6.98
私立學校	348	28.16	349	34.67	351	33.62
私立研究機構	54	20.37	54	25.93	60	15.00

資料來源：2010 年資通安全白皮書。

承上可知，目前政府部門對於個人資料及機密檔案之維護，係電子化政府在推動資訊安全一大課題，資安重要性已成為政府機關不得不重視之一環。

爰此，法務部為使政風機構之運作更具效益，秉持「興利優於防弊」、「預防重於查處」、「服務代替干預」之工作原則，要求各級政風機構加強推動各項重大興利預防措施，期能瞭解發現機關內部問題及癥結所在，促使機關業務標準化、制度化，作業流程公開化、透明化，協助機關建構優質的工作環境。前法務部政風司（廉政署前身，下稱政風司）鑑於政府機關資訊設備常遭駭客入侵擅植網頁、竊取機密資料及作為攻擊跳板等資安事件頻傳，自 88 年 9 月起即依據「行政院及所屬各機關資訊安全管理要點」，請各政風機構協助資訊單位，加強辦理機關資訊稽核工作；另於 94 年 10 月研析資安現況修訂資訊稽核重點，積極協調各機關加強相關資訊機密維護及使用管理稽核工作，全面防範網路洩密事件，落實「稽核資訊安全，防範洩

密風險」之方針。[4]

其中有關政風機構協助執行資訊安全稽核等機密維護作為，亦明文規定於「政風機構維護公務機密作業要點」第 15 點：「政風機構應協調資訊單位建立資訊安全稽核制度，定期或不定期會同相關單位辦理資訊機密維護及稽核使用管理事項。經稽核發現異常者，應即清查其原因及具體事證，依相關法規妥適處理。」，及「行政院及所屬各機關資訊安全管理要點」肆、組織及權責第 9 點：「資訊機密維護及稽核使用管理事項，由政風單位會同相關單位負責辦理。各機關未設置資訊及政風單位者，由機關首長指定適當單位及人員負責辦理。」；同要點第 10 點規定：「各機關對所屬機關(構)資訊作業，應進行定期或不定期之資訊安全稽核。各機關對所屬機關(構)進行外部稽核作業，由資訊單位會同政風單位或稽核單位辦理。」，以為依據。

爰前所述，政風機構加強與資訊單位連繫，係建立網絡聯繫管道及通報機制，強化與民眾個人資料有關之系統使用管理，並定期辦理資安稽核檢查及會同資訊單位辦理資安外部稽核，以確保機關資訊安全。爰此，高雄市政府政風處（以下簡稱政風處）即規劃所屬各政風機構於 100 年辦理 2 次資訊安全專案稽核，以落實資安維護作為。

貳、 現況分析

承前所述，「資通安全」係現階段電子化政府所面臨的一大挑戰。依據國內外的資安事件調查報告所示，資安事件可依資訊安全範圍分成如下幾類：一、網路安全（如竊聽、竄改、阻斷服務等）。二、系統安全（如電腦病毒、網路蠕蟲、後門程式

[4] 政風政策白皮書，2008，27-29。

、木馬、入侵、弱點威脅等)。三、管理安全(不當存取、帳號盜用、未授權登入、社交工程、失竊、資訊資產毀壞)。另依事件發生屬性的方式分類，資安事件又可分成：一、天然災害(因水患、震災、雷擊等天然災害所引起資安事故屬之)。二、人為事故(依來源可分為「內部危安」、「外部入侵」)。三、突發事件(如火警、硬體設備電子損壞、突發斷電等不可抗力之意外事件均屬之)。爰此，不論是系統安全、網路安全或是管理安全的資安事件，除了突發事件為不可抗力因素外，大多屬於人員蓄意或疏失的行為所造成。所以，資通安全除了可以透由資安防護產生預防外，更重要的是啟動管理機制，透過管理層面的控管，降低人為可能發生的資安事件；甚至藉由審視管理面的作業流程，適時修正管理機制，強化實體環境的安全度，提高組織面臨突發事件的應變能力，維持組織的永續營運。[5]

爰上所述，資安管理可謂資訊安全重要之一環，茲就高雄市政府(以下簡稱本府)資訊系統管理現況分述如后。

一、機關電腦資訊系統管理

按高雄市改制後，本府設民政、財政、教育、經濟發展、海洋、農業、觀光、都市發展、工務、水利、社會、勞工、警察、消防、衛生、環境保護、捷運工程、文化、交通、法制、兵役、地政、新聞等 23 局，暨秘書、主計、人事、政風處及研究發展考核、原住民事務、客家事務 3 委員會等共計 31 個一級機關，38 個區公所，153 個附屬機關，合計 222 個機關；另各級學校共 351 所(含空中大學、幼稚園)[6]，行政組織可謂龐大。目前本府行政機關內之資訊系統管控規劃及管理，均由各機關

[5]謝惠玲，2007，＜資訊安全機制規劃及建置之現況調查與分析--以國內大學校園系統為例＞，靜宜大學資訊管理學系碩士論文，14。

[6]高雄市政府人事處全球資訊網，高雄市政府暨所屬機關學校代碼對照表，http://kpd.kcg.gov.tw/archive.aspx?&t=45DA8E73A81D495D&page=3&，100 年 3 月 22 日造訪。

自行處理。又機關內部因業務需要，亦建置有業務資訊系統，如本府工務局違章建築電子化工程管理資訊系統、研考會線上即時服務系統、稅捐處地方稅稅務新平台系統、...等，均與民眾個人資料息息相關，對於資安管理可謂不無重要。

另本府在研考會下設有資訊中心（本府二級機關），並定位為資訊專責機關，其職掌為負責資訊系統規劃、分析設計、開發、建置、推廣、維護管理、相關教育訓練、市政網站服務規劃推動、郵件電子報及垃圾信規劃管理、線上數位學習規劃推廣、設置及應用資訊預算計畫審議、市政共構機房暨相關設備管理、市政網路基礎建設推動服務、資訊安全維護及應變制度推動管理等事項[7]。資訊中心對本府所屬各機關，會定期辦理「社交工程演練」、「學校網站查核」、「網路流量異常、資安預警統計」及「資安事件通報演練」等作為，以預防資安事件發生。

按該中心業務職掌所示，本府各機關資訊業務之維護及規劃，並非由該中心負責，機關內部之資訊系統規劃管控，均由機關自行維護管理。爰此，機關內之電腦系統及設備需有專責單位或專業資訊人才負責，始能針對機關「網路」、「系統」及「管理」等安全技術層面深入規劃與控管，預防可能的資安事件發生。

二、機關資訊專責單位設置現況

按「政風機構維護公務機密作業要點」第 15 點，及「行政院及所屬各機關資訊安全管理要點」第 9 點、第 10 點規定，政風機構應會同或協調資訊單位建立稽核制度。經統計本府所屬各機關發現，僅「高雄市政府民政局」、「高雄市東區稅捐稽徵

[7]高雄市政府公報 99 年冬字第 25 期，462。

處」、「高雄市政府都市發展局」、「高雄市政府工務局」、「高雄市政府警察局」、「高雄市立民生醫院」、「高雄市立聯合醫院」、「高雄市政府捷運工程局」、「高雄市立圖書館」、「高雄市政府交通局」、「高雄市監理處」、「高雄市政府地政局」等 12 個機關設有專責資訊室（科）【以本府設有政風機構之機關為統計標的】（詳如表格 5），[8]其餘承辦資訊業務多為機關秘書室（詳如表格 6）。

表格 5 高雄市政府暨所屬機關設有專責資訊單位一覽表（統計設有政風機構機關）

機關全銜	專責資訊單位	科室名稱	業務職掌
高雄市政府民政局	有	資訊室	
高雄市東區稅捐稽徵處	有	資訊科	
高雄市政府都市發展局	有	資訊室	
高雄市政府工務局	有	資訊室	
高雄市立民生醫院	有	資訊室	
高雄市立聯合醫院	有	資訊室	
高雄市政府捷運工程局	有	資訊室	
高雄市立圖書館	有	資訊組	
高雄市政府交通局	有	資訊室	
高雄市政府地政局	有	資訊室	
高雄市政府警察局	有	資訊室	
高雄市政府地政局鳳山地政事務所	有	資訊課	
高雄市政府秘書處	無	職工管理科	不屬其他各科室業務等事項
高雄市殯葬管理處	無	秘書室	資訊設備管理
高雄市政府財政局	無	公用財產管理科	財產管理資訊系統開發及資訊設備管理
高雄市西區稅捐稽徵處	無	總務室	不屬其他各科、室事務等事項
高雄市政府教育局	無	秘書室	不屬於其他科室事項
高雄市體育處	無	綜合計畫組	資訊管理
高雄市政府經濟發展局	無	秘書室	資訊管理
高雄市政府海洋局	無	秘書室	漁業資訊之設計
高雄市政府農業局	無	秘書室	資訊管理
高雄市動物保護處	無	秘書室	資訊管理
高雄市政府觀光局	無	秘書室	其他不屬各科、室、中心之事項
高雄市政府工務局新建工程處	無	資產管理科	資產管理科資訊設備及系統之管理維護
高雄市政府工務局養護工程處	無	資產管理科	不屬其他各科、廠、室事項。
高雄市政府水利局	無	秘書室	資訊業務
高雄市政府社會局	無	秘書室	各項資訊相關軟硬體設計、規劃、維護
高雄市政府勞工局	無	秘書室	資訊業務
高雄市政府勞工局勞動檢查處	無	秘書室	不屬其他科、室之事項
高雄市政府勞工局訓練就業中心	無	行政組	資訊
高雄市政府消防局	無	救災救護指揮中心	各項資訊系統維護
高雄市政府衛生局	無	企劃室	資訊管理
高雄市立凱旋醫院	無	企劃室	資訊
高雄市立中醫醫院	無	總務室	資訊處理
高雄市政府環境保護局	無	總務室	資訊管理
高雄市政府環境保護局中區資源回收廠	無	總務室	其他不屬各組、室事項
高雄市政府環境保護局南區資源回收廠	無	總務室	其他不屬各組、室事項
高雄市政府文化局	無	秘書室	資訊業務

[8]資料來源：高雄市政府 99 年 12 月 25 日高市府四維人企字第 0990078117 號令(高雄市政府公報 99 年冬字第 25 期)

機關全銜	專責資訊單位	科室名稱	業務職掌
高雄市政府地政局土地開發處	無	秘書室	不屬於其他科、室事項
高雄市政府新聞局	無	秘書室	不屬其他科、室事項。
高雄市政府主計處	無	秘書室	其他不屬各科之事項
高雄市政府人事處	無	秘書室	其他不屬於各科事項
高雄市政府政風處	無	秘書室	其他不屬各科之事項
高雄市鹽埕區公所	無	秘書室	資訊
高雄市鼓山區公所	無	秘書室	資訊
高雄市左營區公所	無	秘書室	不屬其他課、室事項
高雄市楠梓區公所	無	秘書室	不屬其他課、室事項
高雄市三民區公所	無	秘書室	電腦資訊
高雄市新興區公所	無	秘書室	資訊
高雄市前金區公所	無	秘書室	不屬其他課、室事項
高雄市苓雅區公所	無	秘書室	資訊
高雄市前鎮區公所	無	秘書室	資訊
高雄市小港區公所	無	秘書室	不屬其他課、室事項
高雄市鳳山區公所	無	秘書室	不屬其他課、室事項
高雄市岡山區公所	無	秘書室	不屬其他課、室事項
高雄市旗山區公所	無	秘書室	不屬其他課、室事項
高雄市美濃區公所	無	秘書室	不屬其他課、室事項
高雄市林園區公所	無	秘書室	不屬其他課、室事項
高雄市大寮區公所	無	秘書室	不屬其他課、室事項
高雄市大樹區公所	無	秘書室	不屬其他課、室事項
高雄市仁武區公所	無	秘書室	不屬其他課、室事項
高雄市大社區公所	無	秘書室	不屬其他課、室事項
高雄市鳥松區公所	無	秘書室	不屬其他課、室事項
高雄市橋頭區公所	無	秘書室	不屬其他課、室事項
高雄市燕巢區公所	無	秘書室	不屬其他課、室事項
高雄市阿蓮區公所	無	未指定科室	由主任秘書承區長之令，指定人員辦理。
高雄市路竹區公所	無	秘書室	不屬其他課、室事項
高雄市湖內區公所	無	秘書室	不屬其他課、室事項
高雄市茄萣區公所	無	秘書室	不屬其他課、室事項
高雄市彌陀區公所	無	秘書室	不屬其他課、室事項
高雄市梓官區公所	無	秘書室	不屬其他課、室事項
高雄市六龜區公所	無	未指定科室	由主任秘書承區長之令，指定人員辦理。
高雄市內門區公所	無	秘書室	不屬其他課、室事項

資料來源：高雄市政府公報 99 年冬字第 25 期，自行彙整。

承上所述，本府各機關設置資訊專責單位僅為少數，其餘機關多由秘書室承辦資訊業務（如表格 6），對於資訊安全技術面之管控及規劃，尚稱不足，較無法透過技術資源，預防資安事件發生。

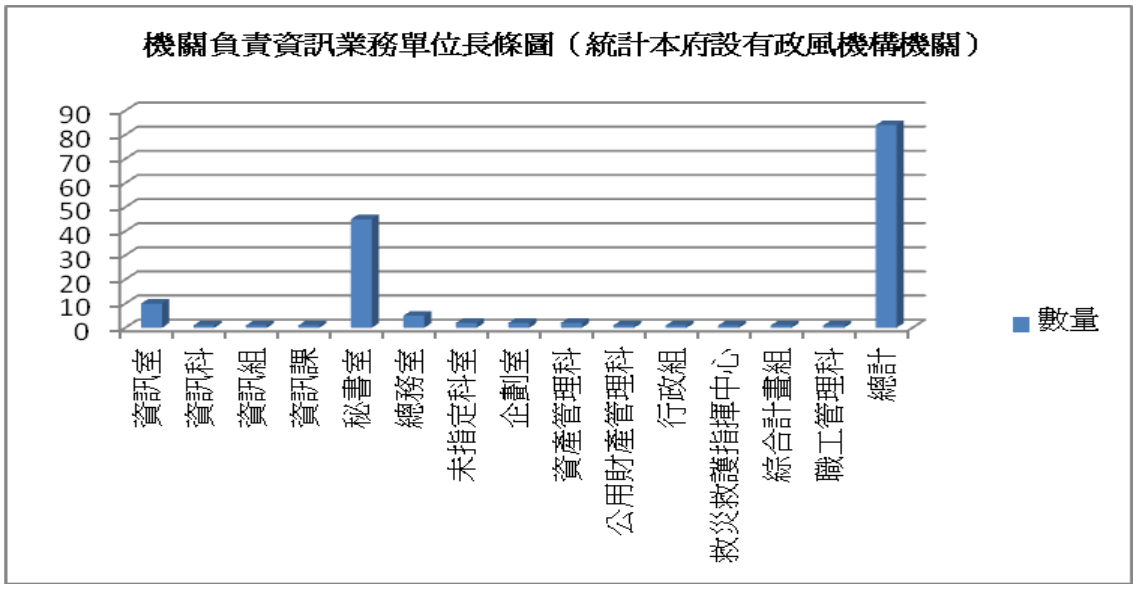
表格 6 機關負責資訊業務單位一覽表（統計本府設有政風機構機關）

承辦機關資訊業務科室	數量
資訊室	10
資訊科	1
資訊組	1
資訊課	1
秘書室	45
總務室	5
未指定科室	2
企劃室	2
資產管理科	2

公用財產管理科	1
行政組	1
救災救護指揮中心	1
綜合計畫組	1
職工管理科	1
總計	84

資料來源：高雄市政府公報 99 年冬字第 25 期，自行彙整。

圖 1 機關負責資訊業務單位統計長條圖（統計設有政風機構機關）



三、各機關政風機構設置現況

按本府各機關有設政風機構僅有 74 個機關（含政風處），相對於本府 222 個機關及各級學校共 351 所[9]，其政風機構設置及人力配置，明顯不足。

表格 7 高雄市政府所屬機關數量與政風機構設置比例

數量 / 組織類別	機關數量	政風機構數量	比例
一級機關	31	24	77.4%
二級機關	153	19	12.4%
區公所	38	30	78.9
學校	351	0	0%
總計	573	73	12.7

[9] 高雄市政府人事處全球資訊網，高雄市政府暨所屬機關學校代碼對照表，http://kpd.kcg.gov.tw/archive.aspx?&t=45DA8E73A81D495D&page=3&，100 年 3 月 22 日造訪。

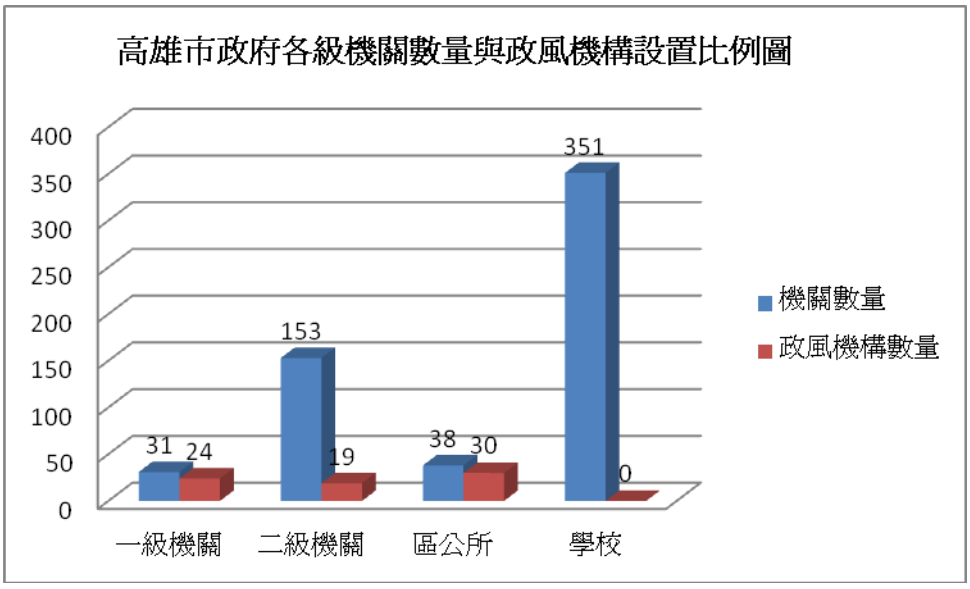


圖 2 高雄市政府各級機關數量與政風機構設置比例圖

其中在學校部份，本文前言中已提及，學校近年來受侵害比例居高不下，雖本府教育局設置有政風機構，但目前各級學校並未有政風機構設置，其政風人力有限，對於所轄之學校，尚無法積極介入有關資訊稽核管理作為，僅能透由學校自行辦理，以為因應。

綜上所述，目前本府雖設有資訊中心，但依行政機關自主性而言，資訊中心並無法介入他機關業務運作，僅能立於協助地位，需透由各機關資訊人員自行管理其資訊系統。另依本府各機關組織編制來看，資訊責專單位及政風機構過少，其中資訊專責單位亦遠低於政風機構。對於法規明定政風機構應配合或協助機關資訊單位辦理資訊稽核業務而言，並無法落實執行。雖目前多由機關政風機構自行或與業管單位配合辦理資訊安全稽核，但僅能針對簡單資訊安全管理作為檢查，對於資訊安全之專業領域，尚無法深入。

參、 100 年度資訊安全專案稽核

政風處為落實本府各機關推動機密維護管理措施，強化與民眾個人資料有關之資訊系統使用管理，業於 99 年 11 月 24 日，函請本府所屬政風機構與資訊單位協調聯繫，加強辦理資安稽核檢查，並將執行成果彙編專案檢查報告。經政風處彙整 100 年度本府所屬各機關政風機構資訊安全稽核成果顯示，目前機關內可能發生資訊安全之態樣及建議事項，分述如后：

一、可能產生危害資訊安全之態樣

（一） 電腦遭植入木馬程式、病毒及 USB 隨身碟有病毒

2008 年間，刑事局偵查發現，駭客集團入侵健保局、教育部，還有多家電信公司資料庫，竊取個人資料，整合成 5 千萬筆名單，再以每筆 3 百元賣給不法集團。甚至連政府官員、民意代表還有企業界人士，都在受害名單內。[10] 爰此可知，駭客入侵電腦最常見手法之一為植入木馬程式。檢查發現，機關之電腦有中毒或遭植入木馬程式之現象，且亦發現 USB 隨身碟有電腦病毒之情事，係對於機關資訊安全一大威脅。

（二） 未訂定資訊安全事件作業規範或自我檢查流於形式

部分機關尚未訂定資訊安全事件緊急應變、通報及回復作業等相關程序規範。另機關辦理定期資訊安全自我檢查（稽核）作業，或同仁自我檢查之作為流於形式，無法落實自我管制。

（三） Windows 作業系統漏洞未定期修補

作業系統和應用程式是十分複雜的軟體，其中可能包含由許多程式設計人員所寫的數百萬行程式，駭客總會想

[10] TVBS 電子報，資料來源：http://www.tvbs.com.tw/news/news_list.asp?no=yehmin20080827001014

盡辦法找出軟體的安全性漏洞來進行攻擊。如果軟體發行後其程式或執行出現安全性漏洞，軟體廠商雖會提供修補程式來處理[11]，但亦可能發生零時差攻擊事件[12]。經檢查發現，部分機關電腦之作業系統並未定期更新修補，可能導致系統出現漏洞，讓駭客針對作業系統漏洞攻擊，導致資安事件發生。

（四） 個人電腦或重要資料未加密或密碼強度[13]不足

承前所述，資安事件發生在人為事故依來源可分為「內部危安」、「外部入侵」，個人電腦或重要資料加密，係為預防機密資料外洩的第一道防線。經檢查發現，尚有人員未於自己電腦設開機密碼，或開機密碼過於簡單或機敏資料未加密等情事，顯見機關人員對於為何設置密碼，及密碼與資訊保密觀念有何關聯之認知不足。

（五） 機關內之公用電腦裝接私人網路使用

機關網路因有資訊人員控管，相關軟硬體防制設備較為完善（如防火牆及防毒軟體），資訊安全性較高。若以公務用電腦裝接私人網路，躲避機關資訊人員管控，而下載非法軟體或至不明網站瀏覽，極易導致公務用電腦中毒，或公務機密及民眾個人資料外洩情事發生，而影響機關資訊安全。

（六） 電子郵件社交工程[14]測試未達標準

本府曾於 100 年度辦理資安攻防演練，惟部分機關開

---

11 資料來源：http://technet.microsoft.com/zh-tw/library/dd548242.aspx。

12 零時差攻擊係指應用程式或系統上被發現具有風險性之弱點後，但是在修正程式發佈之前，或是使用者更新前所進行的惡意攻擊行為，零時差攻擊往往會造成比一般性漏洞更大的危害。

13 密碼強度係指一個密碼被非認證的用戶或計算機破譯的難度。

14.社交工程（socialengineering），通常是利用大眾的疏於防範的小詭計，讓受害者掉入陷阱。該技巧通常以交談、欺騙、假冒或口語用字等方式，從合法用戶中套取用戶系統的秘密。資料來源：http://domynews.blog.ithome.com.tw/post/1252/30016。

啟郵件人數比及點閱連結人數比未達標準。由此可知，本府機關員工對於所謂的社交工程，及其應有之警覺觀念不足，易遭他人以社交工程攻擊，而導致機敏資料外洩之可能。

（七） 電腦主機房安全管控不足

電腦主機房為機關重要資訊系統放置處，若電腦主機房管制不夠嚴謹，遭有心人侵入竊取資料或破壞，則可能造成機敏資料外洩或機關行政業務無法運作之資安事件。檢查發現，部分機關電腦主機房未設置門禁管制規範，亦有機關之電腦主機房未裝設門，無法上鎖管制，且未裝置監視錄影設備，亦有未置滅火器及滅火器過期等情事。

（八） 機關內部網路資源共享區置有個人基本資料

個人基本資料係屬機敏資料，依「電腦處理個人資料保護」規定，不能隨易洩漏。而機關內部網路資源共享區，係機關職員均可存取之資料匣，承辦人員將存有個人基本資料之電子檔，利用此一共享區作為電子檔交換平台，會導致洩漏個人基本資料情事發生。

（九） 公用電腦安裝非合法授權軟體

非正式授權之軟體，可能藏有木馬程式、病毒、蠕蟲等惡意軟體，造成被安裝之電腦感染惡意程式，致洩漏機敏機料。經檢查發現，部分機關同仁會下載非合法授權軟體安裝（例如看圖軟體 ACDsee、防毒軟體 avast、antivrus、影音軟體 cyberlink powerDVD、燒錄軟體 alcohol...等），易形成資安漏洞。

（十） 員工離（停）職或異動後未撤銷或停止該使用者帳號

員工離職（停）職或異動後，對於其因該職位所擁有

之系統權限帳號，應隨職位而更動。本次檢查發現，部分機關有人員職務異動，而成為非授權使用者時，未通知機關資訊系統管理人員撤銷或停用該使用者帳號情形，易發生機敏資安外洩之情事。

（十一） 機關個人電腦紀錄檔（Log File）未另建置存放系統

越來越多的駭客的出現，如何知道自己電腦有無被入侵、資料被下載，可經由查詢電腦的紀錄檔，瞭解電腦使用情形。惟駭客入侵後的第一見事情就是去清理 log，故如何保存一份完整的 log 是非常重要的。資安檢查發現，限於機關資訊系統規劃、管理人才不足及經費短缺，部分機關未建置安全 log 存放系統。

（十二） 學校之網頁在搜尋引擎可搜尋到機敏資料

部分學校之網頁在搜尋引擎可搜尋到學生報名研習營文件、成績系統密碼、印領清冊、獎學金申請名冊及研討會報名等資料。上開電子檔內含個人資料，有外洩個資之虞。

二、預防資安事件發生之建議事項

（一） 定期更新防毒軟體病毒碼及掃毒

為預防電腦病毒及木馬程式之危害，防毒軟體應每日預設時段更新病毒碼，並定期掃毒。

（二） 建立資訊安全事件作業規範，落實自我檢查

增訂或修訂資訊安全事件緊急應變程序規範，並定期辦理資訊安全自我檢查（稽核）工作，以提升資通安全整體防護能力。

（三） 定期修補作業系統漏洞

一般而言，作業系統漏洞係因為軟體寫作產生，故軟

體漏洞修補則需由軟體公司提供新的修補程式，作業系統漏洞才可以修補，一般人並無法自行撰寫修補程式。對於機關同仁來說，僅能請同仁定期上網下載是否有最新軟體修補程式，以為因應。惟若遇有零時差攻擊之情形，一般來講，一般民眾並無法防禦，僅能依靠軟體公司發現，並提供修補程式，或緊急防止措施。

（四） 電腦開機及機敏資料應加密，並視不同需求加強密碼強度

承前所述，政府機關、公立學校資料遭竊或因人為事故發生資安事件情事時有所聞。故對於重要性、敏感性及機密性資料建檔時應加密，以防外洩。另電腦開機系統，亦應設開機密碼，並定期更換，以確保第一道加密防線，惟密碼之強度，應視不同需求加強之。

（五） 訂定資安教育計畫，提升員工資安觀念

訂定資安教育計畫，使同仁接受各項資訊安全課程訓練，有效提升同仁資訊安全觀念及資訊安全維護知能。又資安管理知易行難，除定期訓練外，並應加強宣導，提醒同仁避免因圖一時之方便而造成資訊機密外洩。

（六） 強制規範機關內之公用電腦不能裝接私人網路使用

機關網路因有資訊人員控管，相關軟硬體防制設備較為完善（如防火牆及防毒軟體），資訊安全性較高。若以公務用電腦裝接私人網路，躲避機關資訊人員管控，因而下載非法軟體或至不明網站瀏覽，極易導致公務用電腦中毒、公務機密或民眾個人資料外洩等情事，而影響機關資訊安全。

（七） 設定電子郵件收發功能，預防電子郵件社交工程攻擊

針對電子郵件收發軟體，設定「預覽功能關閉」、「

刪信返回設定」、「開啟封鎖外部圖檔」、「開啟去除Javascript」及「開啓強制純文字」功能，預防人員因不察，而遭受電子郵件社交工程攻擊。

（八） 加強電腦主機房安全管制

應於機關電腦主機房設置進入管制簿，以加強電腦安全性控管。另未裝置有門之主機房，則建議加設門，以便能隨時上鎖，並加裝監視錄影設備，防止資安事件發生。另電腦主機房應設置消防設備，定期檢查消防設備，以為危安狀況發生之因應。

（九） 機敏資料不能放置於機關內部網路共享區

檢查發現置於內部共享區之機敏資料，除請承辦人移除外，並告誡相關人員，不能利用機關內部網路共享區，作為交換機敏資料電子檔之平台，以預防機敏資料外洩。

（十） 禁止安裝非合法授權軟體

為預防機敏資料外洩，機關內之電腦應禁止安裝非合法授權軟體，以預防被植入木馬等後門程式，遭到駭客攻擊發生資安事件。

（十一） 結合人事資料系統，落實職務異動後之權限管制

對於機關員工職務異動後，其系統權限之管制，應結合本府人事資料系統，以電腦管制機關員工職務異動後之權限，避免人力作業可能產生疏漏之情形。

（十二） 建置保存機關電腦使用紀錄檔安全系統

系統被入侵後的第一件事，就是去檢查電腦 log 檔，故應設定一個安全的 log 服務器，讓機關個人電腦使用紀錄檔共同存在同一地方，避免有心人事刪除電腦紀錄檔。

（十三） 清除學校網站放置之個資資料

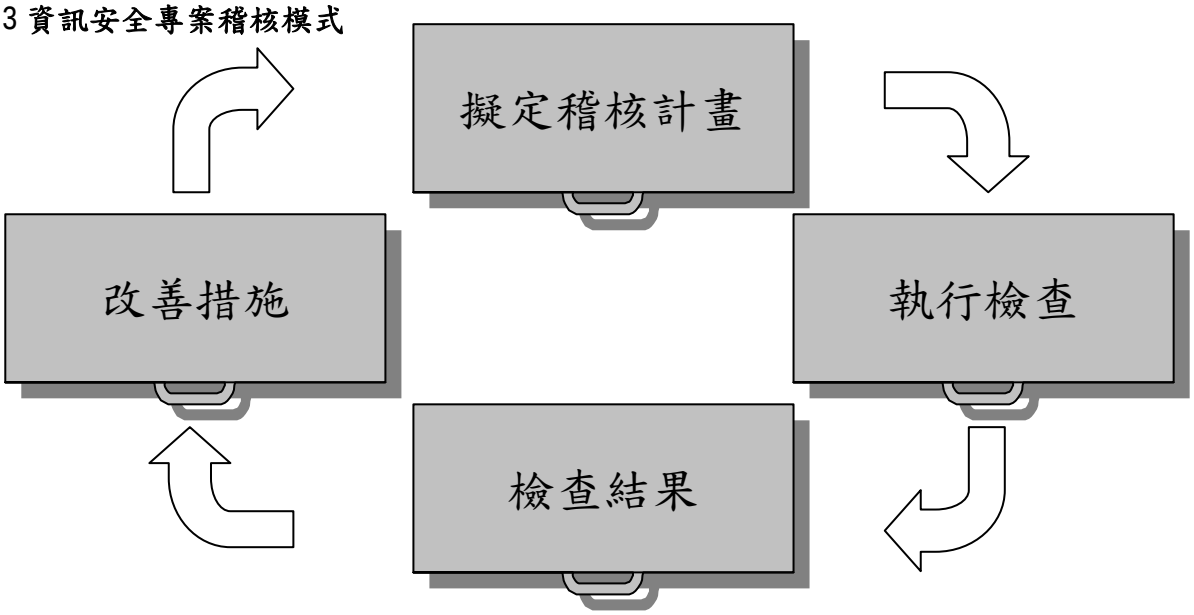
為避免學生個人資料外洩，對於將個人資料放置於網站之學校，均通知該校清除，並告知不可將個資置於網站，以落實公務機密維護作為。

肆、 資訊安全專案稽核執行成效

一、資訊安全專案稽核執行模式

政風處規劃所屬政風機構執行資訊安全專案稽核模式為「擬定計畫」、「執行檢查」、「檢查結果」、「改善措施」等步驟（如圖1）。

圖 3 資訊安全專案稽核模式



爰上所述，茲將政風處暨所屬政風機構辦理100年度資訊安全專案稽核模式，分述如后：

（一） 稽核前

由各機關政風機構衡酌機關特性，除制式之檢查項目外，依機關特性、相關規定或其他管理規定，並參考過去稽核結果，研擬稽核項目，並擬定稽核計畫，簽報機關首長核定後，據以執行。

（二） 稽核中

依據訂定資訊安全稽核項目，備妥機關或受稽單位相關

資訊使用管理規則，協同資訊人員依稽核項目，隨機抽樣進行檢查。另於稽核中提出問題，取得受稽核單位對於稽核項目一致看法，並就相關缺失及疑點，再次進行確認。

（三） 稽核後

針對稽核中所發現之問題，撰寫資訊安全稽核結果報告，簽報機關首長，並移請相關單位檢討改進，並予以列管，持續追蹤改善進度，作為下次稽核之重點。

二、資訊稽核優點

承上所述，政風處暨所屬政風機構辦理 100 年度資訊安全稽核作為之優點分述如后：

（一）對於機關資訊安全之缺失提供建議事項，預防機敏資料外洩情事發生。

（二）進一步瞭解機關內部資訊系統，俾便規劃爾後相關機密維護措施事宜。

（三）透由辦理資訊安全專案稽核，讓機關首長瞭解資訊安全之重要性。

（四）經由資訊安全專案稽核結果產生之建議，讓機關業管單位得爭取購置預防設備之經費。

三、資訊稽核缺失

政風處暨所屬政風機構辦理資訊安全專案稽核雖有上述成效，但亦有下列不足之處，茲臚列如后：

（一）本府各機關未全面設置政風機構，對於透由政風機構協助辦理之資安稽核無法全面落實。

（二）本府各機關設置有資訊專責單位過少，對於更專業的資安稽核項目或資安預防作為無法深入辦理。

（三）機關無資訊專責單位及人才，政風人員對於資訊專業程度亦

不足夠，無法確實針對可能發生之資安態樣稽核檢測，並深入宣導相關資安維護作為。

（四）學校數量太多，以現有教育局政風人力無法全面辦理稽核。

伍、 資訊安全策進作為

承前所述，政風處辦理之資訊稽核雖對於資訊安全維護有其成效，但對於整體資訊安全維護面向僅為其中之一部，故亦有其不足之處。針對政風處 100 年度資訊稽核不足之處，本文研提與資訊安全有關之策進作為臚列如后：

（一）未設置政風機構或資訊專責單位之機關，應每年定期辦理資訊安全專案稽核，並責由機關內部辦理資訊業務之單位負責，落實資訊安全管控作為。

（二）提升政風人員或機關內部辦理資訊業務之人員有關資訊安全及資訊稽核能力，針對可能產生資訊安全態樣之稽核項目查核，並落實宣導資訊安全維護作為。

（三）學校發生資安事件比例較其他機關高，且亦無設置政風機構或資訊人才，故學校應落實有關資訊安全自主檢查，以代替無法辦理全面稽核之窘境。

陸、 結論

在現今網路盛行的時代，各機關學校網站已成為民眾了解市政的重要溝通管道介面，行政機關辦理日常業務，亦離不開電腦及網路系統。惟機關同仁若沒有正確的資安觀念，就無法確實做到安全的電腦防護，網路與現實世界一樣，處處是危機，保持適度的警覺性是必要的。

「資訊安全，人人有責」，目前機關資訊安全最大的危機就是員工不知道危機所在。要做好資訊安全除了技術層面增加系統硬軟體設備外，更需要從內部加強人員的管理及資訊安全之

認知，才能真正落實並有效提升組織整體的資訊安全。（吳倩萍，2006）由此可知，資安稽核固然重要，但提升員工資安觀念、落實資安預防，才能達事半功倍之效。

政風機構自導入「領航管理」觀念後，以逐年建構工作主軸來實現願景（vision），94 年為「溝通觀念、凝聚共識，提升向上、建構優質組織文化」；95 年為「深化核心工作，開創良好績效」；96 年為「強化專業知識，提升組織效能」；97 年為「創新變革，優質治理」；已展現政風新風貌和豐碩亮麗成果。目前政風工作施政主軸，則在「結合網絡，創造價值」，除整合政風體系現有資源，並與不同體系部門跨域結合，建立完善的網絡關係，資訊安全專案稽核即為「結合網絡，創造價值」之具體實現。