臺北縣政府 96 年度自行研究報告

如何提升地政資訊安全管理

研究單位：臺北縣板橋地政事務所
研究人員：鄭鈺訓
研究期程：96 年 1 月 1 日至 96 年 9 月 14 日

臺北縣政府　96　年度自行研究成果摘要表	
計畫名稱	**如何提升地政資訊安全管理**
期程	96 年 1 月 1 日至 96 年 9 月 14 日
經費	無
緣起與目的	透過落實資訊安全管理之各項控管作業，並結合現有的資安防護設備及技術，期能將政府機關面臨網際網路快速發展所造成的資訊外洩及外力攻擊、入侵等資安事件降至最低點，以維護資訊系統之正常運作。
方法與過程	從資訊安全的管理面及作業面角度探討相關之控管措施，並結合現行資安技術及法律規範等層面作全面性之檢討，打造一個更為安全、嚴謹之資訊作業環境。
研究發現及建議	從管理層面做好各項規範、作業標準等基本功夫，並於作業層面輔以相關之資訊設備及資安系統建置，力求做好資訊安全之全面性控管。唯有從全體國民、各企業組織乃至政府機關皆能體認及建立正確的資訊安全防護之道，並遵循相關的法規，才是維護資訊安全之不二法門
備註	

96 年度臺北縣板橋地政事務所專題報告

如何提升地政資訊安全管理

臺北縣板橋地政事務所
報告人：資訊課鄭鈺訓

時間：96 年 9 月 26 日

目　錄

壹、前言

二十一世紀是個網路盛行發展的年代，不僅已成為企業間商務往來的主要交流平台，亦是人們彼此間重要的溝通工具，身為人民公僕的政府行政機關亦不能置身於外，這幾年來紛紛將各項便民服務措施拓展至網際網路作業平台以提供民眾更為便捷的服務；以臺北縣地政機關為例，近年來陸續推辦全縣轄區內二十九個鄉鎮市公所分別設置小而能地政工作站、電傳資訊雙網服務、臺北縣市跨縣市核發謄本服務、法院囑託限制登記網路作業服務、銀行抵押權塗銷網路作業服務、地政電子閘門連線服務、網路申領電子謄本作業服務、跨所申辦簡易案件、北縣地政服務網等業務，提供全縣、全國各類案件申辦、謄本申請及地政諮詢服務，藉由網際網路開放、共通及快速之特性，不僅提供各項地政便民創新服務，更將服務據點拓展、延伸並進而提升政府之施政品質與效率。

然而隨著網際網路之蓬勃發展，資訊之快速交流雖帶來無比的便利，然而其後續引發的安全性與隱密性問題卻一直遭人質疑，也不斷衝擊到企業及政府機關內部資訊之安全保密及個人資料隱私保護問題，且其危害之程度已日趨頻繁、嚴重，有鑒於此，為了確保國家之永續生存發展，不論政府、企業乃至個人皆應妥善保護其資訊系統，落實資訊安全管理，並隨時保持警覺及建立危機意識以面對來自國內

外各種潛在之資訊安全威脅，將資安事件降至最低點以維護系統之正常運作，實為當前最重要、迫切之課題，以下僅就資訊安全其管理面、作業面及相關領域做分析、探討，並提出檢討與建議。

貳、資訊安全管理面探討

資訊安全首重管理，也就是政府部門、企業組織架構及相關之制度是否健全，簡單而言，與人有關的就是管理問題，如果內部之管理未做好，光靠實體安全控管及不斷的採購資安產品是沒有多大效益的，因為往往只要發生一點人為疏失其所造成之損失常讓先前的昂貴的硬體投貲、建設付之一炬。根據台灣與國際間的調查，大部分的資安事件都屬人為疏失或內部管理不當所造成，但是企業或政府行政部門卻花費不少之人力、物力與財力去解決比例較低的外部駭客入侵事件，其實資安產品之防護能力及資安人員技術之養成，以現今為數眾多的資安廠商相繼投入此市場情況下其實並不難達成既定目標，因為各家產品的種類及規格其實大同小異，擁有資源及資安知識亦不難做到，反而是管理層面最容易受忽視，管理嚴謹與否、內部組織與制度是否健全，差異很大，一旦發生資安事件，其造成的資安事件影響就相差很多了。

資訊安全管理最具公信力與典範的首推 BS7799，為英國標準協會所推動之資訊安全管理標準，於 1995 年頒布並於 2005 年改版的 ISO 17799 及 ISO 27001 不僅已成為國際資訊安全管理的準則及規範，更是各國政府單位及企業團體近年來積極導入之資安管理認證，依據中華民國國家資訊基本建設產業發展協進會(NII)於今年 4 月

24 日引述認證機構統計資料指出，目前國內已取得資安管理系統認證的組織共有 124 家，雖然在全球名列前矛，僅次於日本、英國與印度，但政府機構就占了八成，而在缺乏法令等強制性約束力下，企業對資安管理認證並不熱衷，顯示我國政府推動內部資訊安全初具成效，另一方面，卻也代表民間企業對資安管理認證似乎相當興趣缺缺。然而不論政府或民間企業雖然不一定要取得資安認證但仍應需要一套資訊安全管理系統(ISMS)【註】以作為依循的規範，並透過制定嚴謹的資安管理機制才能有效降低或應變未來可能層出不窮的資安風險，ISO 27001 規範共分為 11 個控制目標與措施計有 A.5 安全政策、A.6 資訊安全的組織、A.7 資產管理、A.8 人力資源安全、A.9 實體與環境安全、A.10 資通訊與作業管理、A.11 存取控制、A.12 資訊系統取得、開發及維護、A.13 資安事故管理、A.14 營運持續管理、A.15 符合性，其規劃方法可分為「訂定資訊安全政策」、「界定資安管理範圍(資訊資產)」、「進行風險評估」、「風險管理」、「選定控管目標並執行」，由此可見資訊安全其首要任務即是做好管理面之各項需求，有了妥善的管理、規劃及評估並搭配相關之產品及系統建置才是做好資安管理之不二法門。

【註】ISMS 全名為 Information Secutity Management System，中文譯為資訊安全管理系統是系統對組織敏感資訊進行管理，涉及到人、程式和資訊科技(IT)系統等相關之管控。

以下為針對資訊安全管理層面並參考 ISO27001 相關規範及本縣

地政機關現行管理模式，列舉以下之項目逐一分析：

一、資安政策

行政院於民國 88 年 9 月 15 日訂頒之「行政院及所屬各機關資訊安全管理要點」及民國 88 年 11 月 16 日訂頒之「行政院及所屬各機關資訊安全管理規範」，明定各機關應參考本規範並依實際業務需求訂定資訊安全政策，並以書面、電子或其他方式通知員工及連線作業之公私機構及提供資訊服務之廠商共同遵行。

臺北縣政府地政局及各地政事務所配合本項政策，於民國 93 年 6 月 26 日訂定「臺北縣地政資訊安全政策」及相關規範、要點，釐定資訊安全之定義、目標及範圍等，並定期檢討、評估其可行性及適用性，另亦成立跨課室之資訊安全處理小組，以辦理資訊安全政策之推行、督導及資訊安全責任之分配、協調等事宜。另本縣資訊中心為強化資訊安全管理，亦於 95 年 1 月 2 日簽奉核定「臺北縣政府資訊安全政策」規範相關之存取作業目標、範圍等，確保資料、系統及網路安全，以做為本縣各機關資訊安全管理的參考範本。

二、電腦系統作業程序

參照「行政院及所屬各機關資訊安全管理規範」第肆篇電腦系統安全管理第一之(一)電腦系統作業程序，本縣亦於 93 年 6 月 26 日簽奉核定「臺北縣各地政事務所電腦系統作業程序（範本）」，詳細規範

電腦機房設備操作程序、電腦軟硬體設備作業程序、網路安全管理與維護、其他等相關設備操作程序，透過此規範將各類資訊系統之例行操作與維護程序予以標準化作業。作業程序規範是否嚴謹、人員是否確實依規定程序按表操課，在在影響系統之正常運作與否；以今年 8 月 20 日發生華航公司在日本琉球那霸機場爆炸案為例，及為止擋螺帽、螺栓鬆脫並刺穿油箱導致漏油失火爆炸，而後續的特檢報告亦發現 13 架 737-800 客機中總計 208 組止擋螺絲當中，有一百組出現上緊螺絲的扭力值有「磅數不足」的現象，拴緊螺絲、螺帽，此為一般例行維修作業之標準程序，卻因人為操作上之疏失、不確實而釀成重大意外。

三、文件管理

依「行政院及所屬各機關資訊安全管理規範」之規定，本縣各地政事務所業已配合將各類應用系統之原始程式碼、操作手冊及各項文書作業表單等文件逐項列冊管理，並指派專人保管，具機密性及敏感性文件(如各類系統帳號密碼單)亦放置於專用機房保險櫃，此外各項文件視其重要性亦另行拷貝一份以防不慎毀損等意外，達保存年限之公文等文件亦依規定辦理銷毀作業程序。

四、資料安全

以地政事務所為例，各項主機所儲存資料係為攸關民眾財產之地籍資料，如何妥善保存並做適當之加密處理及異地存放等控管措施，其重要性遠大於一切，資訊設備即使毀損可另行修復或採購，而資料一旦毀損卻又無法即時復原下，所造成的損失是難以彌補的。有鑒於此，本縣亦於 93 年 4 月 15 日訂定「臺北縣各地政事務所資訊儲存媒體安全管理要點」並於 93 年 6 月 26 日簽奉核可，該要點規範資訊儲存媒體使用管理、資訊媒體運送及傳輸管理，例如媒體之保存、攜出、加密、銷毀等程序以保護資料之安全。

五、金鑰管理

配合行政院推動電子化/網路化政府，臺北縣本於地政創新改革、便民的理念，利用政府網際服務網（GSN），規劃電子簽章及電子憑證機制，透過數位電子簽章取代傳統書面文件及簽名、蓋章制度，率先於 91 年 6 月 3 日實施網路申領電子謄本服務，提供線上申辦地籍謄本、規費繳納等網路作業，並藉由建立電子簽章線上認證功能及結合憑證管理，提高資訊與通信安全環境，不僅延伸服務據點，提供更便捷之地政服務，亦保障民眾資料之安全與隱私，大為提升地政為民服務品質及效益。

六、實體安全管理

有鑒於資訊系統的重要性，各項資訊軟硬體設備所在之場所應建置在適當的安全地點並予以保護，本縣各地政事務所已於 82 年起陸續建置專用機房並建置門禁管制設施(含讀卡機等)、監控系統、不斷電設備、穩壓器、空調系統、消防設施、媒體專用保險櫃等，將可能導致火災、煙霧、水、灰塵、震動、化學效應、電力供應、電磁輻射等不良影響及風險納入考量並加以克服以保護各項重要之地政主機、應用伺服器及網路設備等重要設備。以本縣各地政事務所為例，進出電腦機房主控式的外部人員如外單位人員、維護廠商，系統管理人員是否確實辨識身分及記錄進出事由；使用電源延長線是否注意設備負載問題；是否設置防蟲害之設施以防設備、線路受損等。

七、人員資源安全及教育訓練

資訊安全之落實非僅資訊安全推動小組或資訊部門的事，而是全體機關同仁包含高層決策主管所應共同努力、遵循之重要事項，資訊部門人員負責資安政策擬定、技術規範研議、系統建置等工作，而整體之資料及資訊系統之安全需求、使用管理及保護應由相關之業務單負責辦理，唯有彼此相互分工合作才能徹底防範資安事件之發生，此外各機關應定期辦理員工資安教育訓練以提升全體人員之安全意識，本所亦於近年來每年至少舉辦一次全所同仁資安宣導講習，並透

過線上測驗方式，加強同仁之資訊安全意識及個人資訊保護能力。對於人員進用、工作及任務指派時，亦審慎評估其適任性並進行必要之考核。以今年 8 月發生於台南市某地政事務所員工勾結廠商詐領地政謄本規費案，即是對於員工平日工作未盡督導、考核之責致生舞弊情事。

八、監控與稽核

各項應用系統與主機運作一段時日後，因系統本身存在之弱點與設計不良導致可能產生安全上的問題，故系統管理人員應定期保存相關記錄與日誌，並列印稽核報表以了解各項地政應用系統潛在的問題與風險。

另因應使用者存取、使用各項設備與系統的過程，亦應保留其操作、交易記錄並列印稽核報表，以了解是否因外部不當存取影響系統正常運作，作為事前預防、事後補強之因應之道。

本縣各地政事務所系統管理人員針對前開各項軟硬體資訊系統皆配合保存系統紀錄及產製相關稽核報表，並定期呈報上級主管，遇有異常之處隨時作政策檢討、修正，以將資安事件降至最低點。

九、災害復原及事件應變

針對國內外陸續發生之資安事件或系統異常所導致之業務停頓

等重大事故造成之災難，本縣未雨綢繆於 93 年訂定電腦系統異常中斷復原及緊急應變標準作業程序，規範各種防備措施（含人工復原演練），以因應突發之資安危機造成之系統中斷，透過一套緊急應變計畫標準作業流程，建立齊一之標準作業程序，並立即啟動緊急應變機制以使系統儘速回復正常運作，將中斷程序降至最低點，此外臺北縣政府及行政院國家資通安全會報自 93 年起，亦陸續於每年 7 至 10 月左右分階段進行年度資安攻防演練，期藉由此演練措施加強政府機關之資安防護意識及能力。

十、網路實體隔離

鑒於近年網路駭客入侵竊取資料手法越來越純熟、猛烈，行政院於 95 年 6 月 30 日宣布政府機關為確保資料防護，並於 8 月底前落實機密資料實體隔離的資安措施，存放像是民眾個人資料、政府單位機密文件等重要資料的電腦，將限制連結對外網路，同時該電腦在只可連結內部網路的同時，傳輸檔案時都必須透過加解密的機制，連結至網際網路與執行機密或關鍵性業務所在之網路彼此做實體區隔，分別使用不同之實體線路以避免異常入侵事件或異常連線封包，導致重要之資料遭竊或毀損。

所謂「實體隔離」指的是讓使用者電腦無法連結到目標網路，其作法有多種，視各機關之業務種類與連線方式而有不同之因應方式，

以台北縣各地政事務所而言，多年前即採地政內網與連結網際網路之外網彼此以不同線路做實體隔離。一般而言位於地政內網所在之電腦僅單純執行地政相關業務之連線而無法連結至外部 Internet，而連結至外部 Internet 之外網電腦亦不執行地政業務連線作業，藉此方式保護重要地政資料免遭駭客入侵竊取。經此實體隔離方式成效大為顯著，降低地政網路遭外部病毒或後門程式感染入侵之機率。

十一、持續作業與永續經營

為維持政府機關各項便民服務能永續運作，免受外力不當入侵或系統運作錯誤而中斷，本縣及所屬各地政事務所針對地政資訊整合系統有關之各項通訊網路設施、電腦軟硬體設備皆委商辦理維護，而重要之電腦、網路通信設備及資料庫儲存體（如光碟櫃或磁碟陣列）等另與產物保險公司簽訂電子設備綜合保險合約，此外並架設局所間數據專線並考量網路服務中斷狀況申請雙線互為備援，架設防火牆以防外部非法入侵，定期每六個月查核資訊業務乙次並每年檢討增修各項應用系統功能，同時依資訊設施使用期限辦理設施更新汰換。其他如地政電傳資訊系統、地政電子閘門、地政資訊服務網，亦採 BO 機制與 ISP 廠商簽訂合作發展契約提供地政資訊網收後續營運服務或成立相關之維運小組，透過架設 WEB 伺服主機提供各項服務，期由專業之委外廠商及資訊人員優異之資訊技術能力，並配合多台伺服主機

及雙線路互為備援等機制以確保地政業務能永續營運。

十二、委外管理

鑑於資訊人力之不足乃多數政府機關資訊部門所共同遭遇問題，大多之資訊人員多數時間必須花費在行政、公文處理等作業，真正投入於資訊技術之時間仍顯不足，常常購買相關之產品卻苦於無充裕的時間建置或維護，造成投資之浪費。本縣資訊中心率先以整體委外服務的概念，由委外廠商提供必要的軟硬體設備及維運人力，完成全縣電腦病毒防禦、監控及維運體系的建構，並透過「資安監控中心」(SOC) 7x24【註】全年無休的資安監控服務，即便有病毒或後門程式入侵，亦能在最短期間發現並予以清除或隔離，藉此資安委外管理模式並委由專業廠商優異技術能力，期能將資訊安全保全作業做到滴水不漏之境界。

資料來源：資安人雜誌「資安兵法 2006」第 38 至 45 頁(台北縣資訊集中效率、資安兩相得)

【註】SOC 為 Security Operation Center 縮寫，為資安監控中心，由一群全年無休、輪班於嚴格控管的機房中，負責監控各機關或企業組織的防火牆、入侵偵測設備及網路連線狀況，並提供資安的諮詢服務及緊急狀況之疑難排除的專業人員。

十三、預算管理

本縣地政局及各地政事務所於每年年中皆會規劃、編列明年度相關的資訊預算，地所人員平時應隨時注意資訊安全之最新動態、發展，包含國內外重大的資安事件是否可能因現有資訊系統潛在之弱點

而同樣發生於所內，業界最新的科技突破是否可適用於現有資訊設備，倘功能不足是否有迫切需要來編列預算建置；另外當完成採購案後，後續設備、系統之維護與未來擴充性是否一併於年度預算編列時考量進去，本縣資安系統之建置未來雖會朝向由北縣資訊中心統籌規劃、評估、辦理，惟針對地政機關或地所其地政專業領域之系統、異質平台之特性，資訊相關人員仍應審慎評估相關資安系統建置之必要性，並於年度預算編列時納入考量以保護地政機關之資產。

十四、法律遵循

我國立法院在 2003 年 6 月順利修正「刑法」，增設「妨害電腦使用罪章」，將網路入侵犯罪正式納入刑罰體系；而賦予民眾個人資料自主權的個人資料保護法亦於行政院於 93 年 9 月 8 號通過「個人資料保護法草案」。

以網際網路具有匿名性、傳輸環境開放性及作業系統安全維護不易等特質，在檢討各式各樣的資安問題後，可發現大眾對資訊安全意識的淡薄是讓有心人士有機可乘的主要因素。因此，如何加強民眾對資訊安全重要性的認識，以全民之力護衛網路環境已成為各國政府努力的目標。透過對相關案例的分析與學習，建立網路環境應有的法治概念，應是凝聚民眾資訊安全意識，預防網路犯罪的重要關鍵。地所同仁平時亦應注意政府頒訂之相關資安法規，並落實於日常之資訊系

統使用原則，養成良好的操作習慣及資安觀念，並避免誤觸法網。

叁、資訊安全作業面探討

資訊安全之管理，除須於管理層面做好各項規劃、評估及控管外，於實務之作業層面亦應配合完善之資訊軟硬體系統、相關之資安產品及網路環境等建置，二者相輔相成，才能將資安控管做得完整。資訊安全作業面之建置可分以下幾個層面：

一、系統管理

又可細分以下幾個項目

1、主機及伺服器管理

以地政事務所作業環境而言，此類設備一般而言係為儲存重要之地政資料庫或應用系統，以提供使用者遠端存取，故其所含之使用者登入帳號、資料庫權限、資料儲存方式是否做妥善控管，儲存之磁性媒體是否採容錯設計，此外提供外部網際網路服務之功能如網頁伺服器(Web Server)、檔案傳輸伺服器(Ftp Server)、郵件伺服器(Mail Server)等是否採用安全性較高之產品，並定期更新修復程式以免遭駭客入侵，另外是否設定集中控管之管理及程核原則（如 Windows 平台之 AD 網域控制器及群組原則）以有效管理用者連線之方式及紀錄供日後追跡稽核。

2、使用者管理

針對一般之使用者電腦，終端機是否採用以下之控管方式：

(1) 單一登入方式（例如以網域登入）連線至主機或伺服器。

(2) 控管連結至遠端 Server 之權限如檔案、印表機列印。

(3) 對於本機電腦之權限是否依其作業性質設定適當之權限。

(4) 安裝防毒及防駭軟體。

(5) 定期更新漏洞修復程式。

(6) 啟用螢幕保護功能

(7) 控管攜帶型儲存裝置如隨身碟、燒錄器、PDA 等設備之連結電腦功能。

(8) 連結 Internet 之應用軟體及瀏覽器是否設定較高之安全性原則。

3、資料庫安全

以地政事務所為例，地政資料庫儲存人民之地籍財產資料，一旦遭竊取或竄改，其影響民眾權益甚鉅，故地政系統相關之資料庫皆應設定較高之安全控管原則，例如帳號、密碼使用及權限皆要設定較嚴謹之存取方式以免遭不當登入，儲存資料庫之磁性媒體是否採容錯式設計以維持資料之可用性、可靠度，並考慮未來之擴充能力，是否啟用稽核功能以利事後追踪，資料庫系統設計是否採用較嚴謹之設計，如欄位格式設計、建立索引鍵、參考完整性輸入方式等。總之將資料

庫之存取過程控管得愈嚴謹，對資料之完整性、可用性、穩定性與安全性絕對是正面之助益。

4、組態管理

不管是主機、應用伺服器、個人電腦甚至網路設備，如防火牆、路由器、IDP（入侵偵測防禦系統）等皆有組態設定檔以維持系統之正常運作，最典型如 Unix 系統之各類組態檔如密碼設定檔、印表列印、網路組態設定等，其他如 Windows 系統之登錄組態檔（Windows Registry）、防火牆系統組態檔及存取規則設定檔等，此類檔案有的以文字檔或以編碼過之格式存在，不論以何種格式儲存，系統管理人員皆應養成定期備份之習慣，以備將來不慎遭毀損時能快速還原。

5、備份管理

重要之資料如地政事務所管轄之地政系統資料庫、地籍圖庫、建物成果圖檔、公文建檔目錄、登記簿掃描圖檔等，皆與民眾財產悠關，民眾申辦各類案件、謄本等作業賴以地政資料庫之完整性、正確性與穩定性以提供優質之便民服務，故身為系統管理人員應妥善擬定一套備份資料之完整策略，諸如何時做完整備份、異動備份，採用主機異地備援及磁性媒體異地存放之方式，備份之媒體之使用年限、存取速度、保留幾代等因素，是否定期做資料復原演練以當資料毀損時能快

速有效地復原資料，降低民眾之損失。

6、弱點管理

針對主機、伺服器等系統之潛在弱點、風險是否定期做評估並更新修補程式，例如 Windows 系統作業平台，長期以來即存有很多資安漏洞，應隨時注意微軟網站發佈漏洞修補之消息並即時更新，此外針對其他相關產品、設備，廠商有發佈相關之更新程式皆應隨時下載更新，倘預算可行，可採購企業版弱點掃描軟體以偵測並掌握機關內部之弱點風險，並尋求修補補強之策略。

二、網路管理

1、網路設備管理

網路設備種類繁多，功能亦各有其擅長之處，例如應用層負截平衡交換器專司伺服主機之負責平衡，交換式集線器負責資料之傳輸、轉送，路由器專司資料之交換，防火牆專司網路封包與連線之異常偵測攔截，IDS/IDP 專精於應用層內容之入侵偵測與防禦、防毒牆專司病毒之偵測與清除等等，不管如何，以上這些網路設備就是要做好資料於不同網段、不同位置、不同作業平台之同、異質環境下皆能正常傳送、交換，並免於外部駭客之不法入侵、破壞，是故 MIS 人員應就前述設備之特性，妥善予以設定以發揮其最大功能。本縣各地政事務所為有效管理所內網路各項資源使用並防範內、外部不法入侵，除

採購路由器、防火牆並做相關設定外，於內部並建置核心骨幹交換器(Core Switch)，並以雙線串連其下之交換器以達擴充網路頻寬及互為備援線路，至於 IDS/IDP 入侵偵測與防禦、防毒牆等設備，囿於經費有限無法採購，未來本縣資訊中心將統籌納入規劃並已委外管理模式以達集中式控管目標。

2、線路管理

各種不同之網路設備彼此串接時皆透過各種線路予以連結，例如內部區域網路設備可以 RJ-45 接頭之 CAT5、6 線材或光纖線彼此相連，重要之核心交換器度（Core Switch）彼此可以多重線路做串接（trunk）以提升傳輸頻寬及互為備援使用，對外連線可採 E1 專線或 Frame Relay,ADSL 等線路，並建置多條備援線路以提供永不中斷之連線。本縣各地政事務所目前路由器連結外部是以 E1 專線及 ISDN 線路互為備援。

3、網路埠管理

一般而言區域網路所在之網路節點皆可允許使用者電腦透過網路線連接方式而登入網路環境，然而當未受安全控管之電腦（例如未安裝防毒軟體之筆記型電腦）擅自接到某一網路節點時，病毒或後門程式即可能透過該對應網路埠擴散至整個網路，其危害將是全面性而

難以短時間消滅，故近年來網路設備製造商皆有針對網路埠做安全控管功能，例如可設定 mirror port 功能、鎖定 MAC 位址連線控管功能、網路頻寬及流量控管功能等，皆是著眼於網路安全管理而設計，系統人員針對此項功能尤應嚴加控管以杜絕內部不當連線造成之資安事件。

4、IP 位址管理

IP 位址猶如電腦之身份証，網路上每台資訊設備皆有獨一無二的 IP 位址以做為彼此辯識使用，IP 位址控管不當，例如重覆使用、遮罩位元設定錯誤，皆可能導致無法存取網路，甚至造成網路塞車，此外當 IP 位址不敷使用時，亦應考慮使用另一網段並作轉址之設計以維持網路之正常運作，或用主機標題名稱以從同一 IP 位址管理多個網站。本所因資訊設備繁多，同一網段之 IP 已不敷使用故針對 IP 不敷分配之課室電腦配置另一網段 IP 並作轉址功能以連結地政系統網路。

5、DNS 管理

隨寬頻時代之來臨，網際網路逐漸從學術研究單位延伸到企業、家庭以及個人。使用網路的人口對 Domain Name 的需求，也隨著寬頻上網環境的普及而快速增加。DNS 為網際網路之重要基礎建設，

良好的 DNS 設定及管理能有效增進網路資源之利用；相對的，不良的 DNS 設定則會消耗網路頻寬及系統資源，影響網路的品質與正確性。因此，如何正確而有效地建置 DNS 以及維護 DNS 的穩定運作，讓全國網路使用者有一個良好的 DNS 環境，促進網際網路資源的廣泛應用，成為網路國度裡最重要的課題之一。

本縣各地政事務所現行建置之網站其網域名稱皆採用向政府網際服務網（GSN）申請政府專用之網域名稱註冊系統所核發，透過政府 GSN 合法核發之 Domain name 及納入縣府共通框架維運管理以提供網站地政便民服務，不僅免除機關自行架設網頁伺服主機、網路設備之硬體及日後維護成本，可大為提高地政事務所網站之穩定度及安全性，而機關僅專注於網頁內容的提供即可，對於網站內容亦可獲得更多元、豐富的資訊。

6、無線網路

無線區網可說是近幾年來竄起最快的新科技，不論自大型企業到中小企業或是家庭用戶，使用無線網路可說已經成為一股風潮。舉凡前幾年推行的 WAP 手機無線上網，到近年來的 GPRS、i-mode 上網等等，都是無線網路嘗試融入我們日常生活的無線網路生活計畫。地政機關為落實行動化政府概念，內政部於 95 年 9 月 22 日推動 PDA

版地政電傳資訊系統服務並推展至全國正式上線使用，後於 96 年 7 月 11 日再推動「PDA 版地政電子謄本服務」全國上線，以無線網路，突破空間限制，以往民眾只要在家中或辦公室，就可申請查詢地籍資料，雖已頗為方便，惟基於迎接無線網路時代來臨，透過建立「行動資訊便民服務」作業模式，讓民眾可隨時隨地經由 PDA 透過無線網路取得地籍(圖)謄本。

在響應政府 M 化台灣(『M-Taiwan』)概念下，地政機關配合推動這些相關之便民措施，讓民眾對於地籍資料之查詢、使用「隨手可得」，徹底顛覆傳統之存取方式，亦突破時空之限制，深獲民眾肯定；然而在享受無線科技帶來的便利性的同時，無線網路產生之電波讓網路上有心人士得以自由截取，造成個人資料隱私外洩等資安問題，如何達到科技的便利性與兼顧安全性的平衡已成為企業及政府於導入無線服務時最大的挑戰。

一般而言使用無線網路設備有以下幾個原則須注意：

(1) 定期更改無線網路設備預設密碼

(2) 盡量不開放遠端管理模式

(3) 隱藏網路 SSID

(4) 控管使用之 MAC 存取列表 (Access Control List)

(5) 盡量採用安全性最高的 WPA 加密認證，以避免讓有心人士破解

(6) 防火牆區隔內外網段，亦即採用內部虛擬 IP 與外部合法 IP 之 NAT 轉址模式

7、網路防禦

隨著資訊科技不斷進步，網路安全威脅已由以前的透過磁片散佈的單一檔案型病毒、巨集病毒、木馬或蠕蟲，逐漸發展為透過網路、網頁、電子郵件散佈的各式變種病毒，近年來更演變為混合式威脅（不再只是單純的病毒、間諜軟體、後門程式）、垃圾郵件、網釣攻擊或網址嫁接等攻擊手法，為了反擊這些不斷翻陳推新的網路威脅，資訊安全供應商的產品也隨需求而演化。市場上一開始出現的是各自獨立運作的防毒軟體、防火牆（軟體式、硬體式）、入侵偵測／防禦系統、內容過濾、反垃圾郵件、反網路釣魚軟體等，而使用者發現這些網路安全設備必須加以整合才能達到完整防禦的效果，因此多半另聘系統整合商將這些軟硬體，連同網路裝置一起「串起來」，以聯合防禦的方式與網路威脅進行攻防戰。幾年前有些廠商開始著手研發將這些不同功能的產品予以整合至同一設備稱為 UTM(Unified Threat Management)，系統使用 ASIC 晶片之硬體加速的 UTM 裝置，可以多重防禦機制同時進行對應的偵測掃瞄，有效地阻止網路威脅侵害；不管採用整合多種設備或是採用 UTM 設備之管理方式，皆應注意以下幾個原則：

(1) 系統之運作效能：

隨時注意系統之運作效能，若發現校能太差，是否有異常之連線或系統整體負荷過重，必要時應請維護廠商協同解決。

(2) 即時有效更新：

定期更新韌體、病毒碼、IPS 入侵特徵碼、反垃圾郵件黑名單等資料

(3) 整合式管理平台：

在單一平台上管理多種網路安全功能，必須有一體化的軟體進行搭配，用戶才能透過此一管理介面有效率管理眾多功能。管理介面整合的範圍相當廣泛，像是網路使用政策 (policy) 的設定、網路使用狀況監控，提供多樣化且具彈性的報表設定等，都能協助用戶完整地掌握網路安全狀態。而遇上具有分散式據點的管理需求時，就必須提供集中管理的對應解決方案，以便進行網路安全政策派送，以及在單一介面統一管理分散的設備等。

(4) 價格功能合理：

除考量設備本身費用外，使用授權費、每年更新各式威脅防禦資料庫的費用，以及其他後續擴充能力與對應的相關維護費用等，亦應一併納入整體預算考量。

8、電腦/數位鑑識

現今網路環境面臨資安威脅越來越高，然而卻有 30%的企業及政府機關並不知道內部究竟有多少資安事件正在發生、產生多少損失及危害程度。企業及政府機關雖已採購安全設備如防毒軟體、防火牆、入侵偵測／防禦系統等來作好防禦，然而即便擁有完善的防禦設備真的能保證對安全嗎？有太多真實案例顯示答案是否定的。因為內憂外患衍生之安全事件，例如內部管理不周或是外部之入侵手法道高一尺魔高一丈，即便是資訊安全專家亦防不勝防，是故如何完整保留入侵之紀錄及犯罪證據以查明入侵來源並找出防範之道，已成為近年來電腦/數位鑑識技術發展之重要因素。

目前業界已陸續開發許多相關產品，並採用最新的網路安全分析技術，除了完整的蒐集所有網路封包並加以解析，亦將不同的安全產品產生的事件紀錄轉換成統一的檔案格式；再利用獨特的網路傳輸紀錄與視覺化的工具，可完整的還原犯罪現場，並找到攻擊來源以作為將來有效的「呈堂証供」，不僅可制裁犯罪者亦可免於機關未來再度遭受相類似之攻擊。

三、應用系統與服務

1、防毒與反間諜軟體

近年來病毒、蠕蟲、後門及間諜程式已呈等比級數及不同混合變種方式透過郵件、網頁傳送等方式不斷在網路上橫行，本縣資訊中心

率先以整體委外服務的作法，由委外廠商提供必要的軟硬體設備及維運人力，完成全縣電腦病毒、後門及間諜程式之防禦、監控，並透過「資安監控中心」(SOC) 7x24 全年無休的資安監控服務，將病毒或後門程式等入侵之機率降到最低點。透過專職、專業廠商集中控管之服務將北縣整體資安管理做到最嚴謹之防護，大為減低各機關以前各自為政、各別管理造成之防護能力參差不齊及未能及時通報上級機關所造成的資安問題。

2、即時通訊及內容過濾管理

隨著網際網路與電子郵件在政府、企業間使用的普及，員工上班時間利用網際網路機率也大為增加。為防止員工利用上班時間瀏覽與業務無關之網站、收取電子郵件或使用 Yahoo!奇摩即時通、微軟 MSN 之類的即時通訊軟體聊天及傳送非關公務的檔案，導致生產力降低、機密資訊外洩風險及浪費網路頻寬，限制員工上網、使用即時通訊軟體或收取電子郵件的工具需求也有增加的趨勢。

市面上已有多家廠商推出之內容過濾軟體，為員工資訊管理（employee information management）的一環，即為解決前述因員工不當使用網路資源所造成的資安問題。內容過濾基本原理及功能是以防堵員工連上名列供應商資料庫的網站 URL、管制使用即時通訊軟體及檔案傳送功能、防止員工利用電子郵件把公司機密資料傳送出去

等，配合相關之監控報表分析，禁止達到事前預防、事中應變，以及事後舉証的多向防堵策略，惟這樣的作法仍有部分違反個人資料隱私保護之爭議，這部份普遍尚未獲得一致的共識。

3、垃圾郵件管理

電子郵件堪稱是網路時代的殺手級應用，對於企業或是個人都是效用極高的訊息傳遞工具，但隨著垃圾郵件的氾濫與其夾帶的威脅，電子郵件已成為現代上班族的夢魘。

目前垃圾郵件的比例已經超過所有信件量的 70%，多數人在收信後需要花費許多時間從收件夾中區分出垃圾郵件並予以刪除，若一不小心即可能誤刪其他重要信件，甚至造成嚴重後果。不過隨著近幾年電子郵件管制法的成形，以及各種垃圾郵件管理解決方案的出爐，垃圾郵件逐漸受到有效的管制，也因此讓網路使用者開始可以有效管理個人郵件氾濫的問題，現行的垃圾郵件防治方案中，普遍是從技術的層面來管理，也有些是從人性面下手，如立法規範或是付費要求等等，但都無法有太好的成效；技術層面作法包括使用黑名單比對、建立白名單列表、關鍵字比對、指紋辨識、啟發式技術以及的貝氏分析過濾法等，一般而言皆可達到不錯的成效，不過仍無法完全阻斷垃圾郵件的騷擾，比較簡單的作法為設定公務往來之聯絡人並訂相關規則存取至對應資料夾，其他位置之郵件則一律忽略或刪除；此外有架設

mail server 之機關尚需注意不要被當成郵件轉寄中繼站(relay server)，造成駭客攻擊之跳板。

4、版權管理

為落實尊重智慧財產權，不論使用之資訊軟硬體設備、文件、媒體等，均應為合法授權使用，本所現行地政系統使用之軟體皆為委商開發或上級機關交付，資訊設備近年來亦統一由北縣辦理租賃案撥付;其餘一般商用業務軟體皆採購合法授權或使用臺北縣政府與廠商簽訂之政府機關大量授權之合法軟體;另各類地政相關系統使用之程式、手冊、文件等亦做分類及版本控管,除能掌控資料的歷程記錄外，亦能落實版權管理。

5、系統開發管理

本縣各地政事務所現行使用之地政應用系統大部分皆為委商開發或上級機關交付,於辦理系統採購時皆於建議書需求說明書中詳列系統需求、功能及目標等，並要求得標廠商需考慮安全的系統設計並提供稽核報表功能及與資訊安全相關之管控、分析模組建置；另廠商亦須簽訂保密協定，不得洩漏機關之各項機密資訊。

肆、網路威脅案例探討

一、2000 年 3 月駭客利用 DDoS【註】的網路攻擊方式，引起 Yahoo、Amazon 、CNN 、eBay 等知名網站癱瘓，以致無法提供正常服務。

【註】DDoS 全名為 distributed denial of service attacks，為 DoS(denial of service attacks)攻擊的一種變形，因為它是透過網路分散來源的技巧，所以將之稱作分散式 DoS（Distributed DoS，簡稱 DDoS）攻擊。
DDoS 攻擊方式在於它是從網路上的許多台主機同時發動類似 DoS 的攻擊行為，所以遭受攻擊的主機同時面對的敵人數目將是數百台來自不同網域的主機，這種獨特之處，使得 DDoS 攻擊不一定要真正把遭攻擊主機的系統程式給異常終止掉，只需要同時送出遠超過網路負
荷或者是遠超過遭攻擊主機所能允許的最大連線數量的資料，就能達到癱瘓目標網站之目的。

二、2001 年 4 月國內首宗網路銀行遭人入侵盜領事件，SSL【註】安全機制受到質疑。

【註】SSL(Secure Socket Layer)是 Netscape 所提出來的資料保密協定，採用了 RC4、MD5，以及 RSA 等加密演算法，將使用者與網站之間所傳的資料使用 SSL 加密協定來保密，除非能破解傳輸密碼，否則其他任何人都無法得到這些機密資料。

三、2001 年 5 月東科大火燒出企業資料異地備援的重要性，也考驗企業災害復原的能力。

四、2001 年 7-8 月紅色警戒 Code Red 電腦病蟲肆虐，造成數十萬台電腦受駭，網路頻寬阻塞：白宮被迫更改網址、商務部暫時關閉公共網站、財政部金融系統停擺等。

五、2002 年 4-5 月國內網路報稅，隱碼攻擊(SQL Injection)【註】問題造成國人對網路報稅的疑慮 。

【註】SQL Injection 是一種未做好輸入查驗(Input Validation)的問題，即在撰寫應用程式時，沒有對使用者的輸入做妥善的過濾與處理，便將其組合成 SQL 指令，傳送給 SQL server 執行。因而若使用者輸入之資料中含有某些對資料庫系統有特殊意義的符號或命令時，便可能讓使用者有機會對資料庫系統下達指令，而造成入侵所帶來的損失。事實上，這樣的疏漏並不是資料庫系統的錯誤，而是程式設計師或軟體開發者的疏忽所產生的。

六、2004 年 6 月全球出現第一隻手機病毒叫食人魚病毒,影響手機正常運作。七、2003 年 4 月建中學生入侵總統府網站，修改首頁。

八、2003 年 6 月刑事局偵九隊日前破獲大學入學考試中心及國中基測電腦系統遭駭客入侵一案，主嫌年僅十九歲，患有自閉症。

九、自 2002 年起陸續透過 MSN【註】傳送傳送病毒訊息

【註】MSN 為 MSN Messenger 簡稱，為微軟提供之一套線上聊天軟體，除了可以透文字傳輸訊息，也可以傳送檔案及張貼有趣的表情符號等強大功能，近年來大受使用者歡迎，因存在安全上漏洞近年來亦成為駭客攻擊目標。

十、2007/04/09 國防大學某主任教官將辦公室使用的 USB【註】隨身碟以及內存機密資料，帶回家中在自家電腦上操作。該隨身碟再被插回到辦公室的電腦，經掃描發現有木馬程式，因而事發。

【註】USB 的規格是由英特爾、國際商業機器公司 (IBM) 、Microsoft、Compaq、Northern Telecom 與 DEC 等全球電腦資訊大廠共同制定出來的傳輸標準，從早期 1995 年 11 月 13 日制定的 USB1.0 規格，可分 12Mbps 的高速傳輸模式(Full-speed)與 1.5 Mbps 的低速傳輸模式(Low-speed)兩種，在高速模式下的資料線長度為 5 公尺，低速模式則只有 3.5 公尺，到了 1999 年 12 月發表 USB2.0 的 0.9 版將傳輸速度推向 480Mbps 之超高速境界。此

外，使用 USB 作為資料 (Data) 傳輸介面的周邊產品，都具有隨插即用 (PNP) 及熱插熱拔 (Hot insertion, hot swapping) 等相當便利的功能。

十一、2007/04/13 警局傳出筆錄因 P2P【註】軟體使用不當而外洩的事件，凸顯了 P2P 軟體在方便之外的安全威脅問題。

【註】P2P 全名為 Peer to Peer，為一種點對點通訊傳輸工具，傳統 HTTP/FTP 傳送檔案方式，採用戶與主機的通訊模式(Client-Server Mode)，P2P 檔案傳送方式，採取用戶與用戶的通訊模式，依其設計的功能，每個使用者在利用此軟體下載他人資料的同時又可分享自己資料供他人下載，因可以同時連接多個下載點，分散式下載檔案，因此下載的人越多，速度越快，此一特性使 P2P 軟體推出以來成為網路上資料交換相當受歡迎的工具。惟因採非集中控管方式進行資料傳輸，安全性較差近年來亦成為駭客攻擊目標。

十二、2007/09/12 點對點(P2P)網路電話軟體 Skype【註】亦成為病毒傳送媒介該蠕蟲會偽裝熟人向使用者打招呼，並傳送內含惡意軟體的網站連結。【註】Skype 是一種支援語音通訊的即時通訊軟體，在網路上利用點對點技術與其他用戶連結，可進行高清晰的語音聊天，Skype 在台灣與 PChome Online 合作，推出的 Skype 又可稱為 PChome-Skype。主要功能可撥打至一般市話、手機、國際電話，藉由網際網路的傳輸可省去話務傳輸成本，因此費用較低，目前網路對網路撥打免費，撥打到台灣、美加等地市話 0.69 元／分，比台灣長途市話 2.1 元／分便宜許多。

資料來源：2002 資安法律案例彙編第 1 輯.pdf、2003 資安法律案例彙編第 2 輯.pdf、2004 資安法律案例彙編第 3 輯.pdf、2005 資安法律案例彙編第 4 輯.pdf、2006 資安法律案例彙編第 5 輯.pdf

伍、地政資訊安全管理問題檢討與建議

近幾年來，透過網際網路，人們可以瀏覽國際、政治、財經、科技、學術、消費、娛樂等各類資訊，滿足知識與實用上的需求。但除聯絡溝通的功用外，網際網路更已成為國家許多基礎建設的載具。從水電的供輸、稅賦的報繳、到交通運輸的帷幄等，皆已不復全賴人工處理。但誠如水能載舟，亦能覆舟，網際網路雖為人們生活帶來無比的便利，卻亦成為犯罪者的溫床，稍有不慎，將為社會、國家的發展帶來重大影響，其危害程度亦難以估計。如何做好並有效提升資訊安全管理工作是現今不可忽略之課題。

資訊安全之管理廣泛而繁雜，尤其是近來駭客技術更加精進，入侵手法不斷推陳出新且破壞性更大，而拜網路之暢行無阻，不分國界與族群之特性，加上駭客工具程式愈來愈容易取得，而相關之資訊設備或系統於研發設計時亦不可能做到百分之百之安全；綜合以上原因，電腦一連上網路極可能中毒或遭入侵，在無法保證所使用資訊系統的絕對安全下，如何做好基本防護之道以降低資安事件發生的機率，是任何電腦使用者必須面對之首要任務；爰此，本縣地政機關近年來除善加利用資訊科技快速發展及網路開放、多元化之優勢，不斷亟思開創各項創新服務，對於逐漸全面導入網際網路連線服務之各項地政資訊系統及設備，亦不遺餘力的投入相當之人力、設備與經費

等，除了從管理層面做好各項規範、作業標準等基本功夫，並於作業層面輔以相關之資訊設備及資安系統建置，力求做好資訊安全之全面性控管。

然而本縣各地政事務所於現行地政資訊管理實務上仍面臨以下之安全風險，相關可行的建議亦如下分析：

一、 本縣各地政事務所現有之機房管理人員限於組織、人員編制，多半為從地政人員轉任或為約聘雇人員，資訊本職系之人員仍屬少數；以非資訊相關職系之人員從事資訊系統管理工作，雖可藉由資深的系管人員作經驗傳承或透過一連串之教育訓練與研習會等課程獲取資訊專業知識與技能，然以地政業務近年不斷規劃各項創新服務，並積極導入網際網路作業平台，相關的軟硬體系統如資料庫主機、網路設備、地政業務各資料庫系統及各項相關應用伺服器與網路服務等之建置環境亦隨之益加複雜與異質化(例如不同之資料庫系統、不同之登入網路環境方式等)，在在增加系管人員管理上的之負擔；再者，以現行地政機關開辦的各項資訊教育訓練仍以偏向實務之操作面，對於教授理論基礎、觀念與管理面之課程並不多亦不夠深入，尤其是網路相關設備如路由器、交換器等，本縣各地政機關雖有與廠商簽訂各項資訊系統維護、諮詢合約，委由廠商做各項系統例行

維護及異常診斷、處理等相關服務，然而屬地政資料較為機密、敏感性質者仍應由地所系管人員負責，不宜由委外廠商經手、維護以免衍生資訊外洩等資安事件；綜合以上因素，以現今地政資訊日益龐大而複雜之作業環境，對於系管人員尤其是地政人員轉任者，更加面臨管理、維護上之壓力與瓶頸，地政機關雖有設置職務代理人制度，可降低管理之風險，然以地所現有人力普遍不足情況下，機房人員仍面臨人員短缺現象，遇系統異常之緊急狀況下，該等系管人員仍須設法排除問題，無形中增加管理之風險。對於以上人力資源之教育與管理上，建議以下相關之作法：

1、因應地政資訊業務之日益多元化、複雜化，地所系管人員之工作執掌分工愈加細密之趨勢下，對於未來地政資訊業務更加深化與全面化之潮流下，資訊職系之系管人員其專業技能應予重視，未來倘組織編制許可下，應酌予增加資訊專職人員名額以提升資訊管理之品質與效率。

2、未來規劃資訊系統相關課程時，應特別針對地政人員轉任之系管人員，加強前開所述之資訊軟硬體系統課程內容之深度，課程之安排應按步就緒，從基礎至進階，循序漸進並搭配實際業務使用之建置環境做實機演練，使理論與實務能有

效整合，提高學習成效以為未來管理各項資訊系統之有力基礎。

二、 本縣地政機關自 93 年 1 月 2 日起開辦全縣跨所申辦簡易案件以來，雖為全國地政機關首創之舉，不僅大為降低民眾洽公往返的時間及金錢，無形中亦拓展了地政便民服務的據點，然而現行跨所連線架構上本質上屬於高風險之資料存取方式，加以地所現今使用之地政整合系統因為內政部統一委商開發並發交全國各地政機關使用，因原系統設計之初不夠嚴謹，部分程式存有安全上漏洞導致主機資料庫部份物件須配合做相關設定以為因應，本縣地政團隊已於近年來陸續蒐集相關設計不當之程式並呈報內政部中部辦公室，目前亦已成立專案小組，正積極全面清查所有後端主機資料庫存在之資安風險問題，未來期待上級主管機關及維護廠商能加快腳步配合做相關系統修正，使本縣現行推辦之各項網路便民服務系統不僅在資料存取上更加便利，又能兼顧資料使用安全。

三、 本縣地政機關在對外網路連線上雖採地政內網與連結網際網路之外網彼此以不同線路做實體隔離方式，然而從使用者端乃至各項應用伺服主機幾乎皆採微軟之 Windows 系統平台，該系統在目前市場之佔有率雖仍獨佔鰲頭，但因該系統設計不夠嚴

謹，長期以來即存有很多資安漏洞。本縣資訊中心雖已將防毒業務採集中委外管理方式並全面建置於本縣所有機關(含本縣地政局及各地政事務所)，然而外部之駭客攻擊手法及能力卻日益精進，所謂道高一尺，魔高一丈，尤其近年來更主動出擊，一旦發現 Windows 系統存在之大小安全弱點，即以零時差之方式攻擊，在還未及於第一時間修補漏洞程式之受害電腦散佈病毒與惡意程式，或藉由網路釣魚(phising)、社交工程手法藉機破壞與竊取電腦內部及使用者個人資料，而這些攻擊行為常常都是防毒軟體無法主動偵測到或是已偵測到卻未能有效清除或隔離，讓系統管理人員防不勝防，本縣各地政機關雖已於內外網配合建置 Windows 漏洞修補更新系統，然因作業系統本身潛在之弱點風險隨時易遭有心人士攻擊，是已目前即使是資安專家亦仍無法全面有效防堵此類病毒及攻擊程式之安全威脅。在無法保證連結網路後做到絕對安全前提下，如何於自身及教導使用者降低使用電腦之威脅，以下建議幾點供參：

1、定期注意微軟發佈的最新安全漏洞訊息，並配合檢視內部之電腦是否及時更新。

2、定期檢視防毒伺服主機之病毒、惡意程式紀錄，一經發現異常病毒感染或攻擊事件應即刻至受害電腦做必要處置(例如拔

除網路線，重新以安全模式掃毒以徹底清除威脅)，以避免災情擴大；若仍無法有效修復，應儘速通知委外防毒廠商尋求協助、解決，必要時應將該電腦作系統重建以有效清除安全威脅。

3、對於使用者上網的行為例如連結非關公務網站或是使用網頁型郵件服務收取個人信件等皆應加以限制，此外如使用傳訊軟體如微軟 MSN、Yahoo!奇摩即時通等皆應從嚴控管；諸如以上之存取網際網路方式皆是駭客最常攻擊的模式，以內政部中部辦公室委商開發的「地政資訊網路訊息平台」為例，該系統為提供全國地政人員公務上聯絡、溝通的一個管道、平台，系統雖採憑證控管以辨識身分之機制，然對於在網路傳遞之訊息內容或檔案傳輸並未採資料加密、簽章等安全控管措施，恐有資料外洩之虞，故建議地所人員儘量不要將地政敏感或具機密性質的資料發布於該系統上(否則亦須採用較為安全之代號或密語表示)。另對於公務上收發電子郵件的使用者，因其電腦可能存在之大量垃圾郵件及其衍生的夾帶病毒、後門程式及網路釣魚等資安威脅事件，為面臨資安事件高風險所有人，應加強宣導應有之防範之道，隨時提高警覺，對於來路不明的郵件最好直接予以刪除，以徹底杜絕威脅的

來源。

四、本縣地政局及各地政事務所於每年年中皆會規劃、編列明年度相關的資訊安全預算，然相關預算或限於縣府財政預算分配，或上級主管機關考量等因素，經常被大幅刪減；本縣資安系統之建置未來雖會朝向由北縣資訊中心統籌規劃、評估、辦理，惟針對地政機關其地政專業領域之系統、異質平台之特性及所處理之地籍資料龐大、複雜度、及時性與不容有絲毫錯誤等特性，皆非本縣其他機關所能比擬，而屬地政資訊安全領域的相關設備、系統之規劃、投資良善與否，在在攸關民眾地籍財產權益，這些涉及地政資料處理、運算所需之軟硬體設備亦已完全整合於網際網路之作業平台，處於無可避免的安全威脅下，更須予以有效保護，諸如此現實狀況亦非資訊中心所能完全理解、掌控，建議未來在年度編列預算時，能更加積極與資訊中心及相關審議預算之上級機關溝通，在了解地政機關處理地籍資料之重要性、及時性與相關建置系統之複雜性、異質性，未來不管是統籌由縣府作資安預算規劃與建置或由地政機關自行編列、規劃，在取得高度共識下，希望所投資的資安相關設備皆能適切的發揮其應有功能，所謂工欲善其事必先利其器，在完善的組織制度管理下，配合這些資安利器，期能將本縣地政機關之資訊安全工作提升至更高的水準。

陸、參考文獻

1、行政院及所屬各機關資訊安全管理要點.doc(88 年 9 月 15 日訂頒)

2、行政院及所屬各機關資訊安全管理規範.pdf(88 年 11 月 16 日訂頒)

3、資安人雜誌-資安兵法部署二○○六

4、資通安全法律案例宣導彙編第 1 輯(91 年 6 月)

5、資通安全法律案例宣導彙編第 2 輯(92 年 6 月)

6、資通安全法律案例宣導彙編第 3 輯(93 年 6 月)

7、資通安全法律案例宣導彙編第 4 輯(94 年 6 月)

8、資通安全法律案例宣導彙編第 5 輯(96 年 6 月)

9、資訊安全與管理簡報講義(報告人:行政院研考會孫百佑,94 年 9 月)

10、(96)臺北縣公務人員訓練班 ISO27001 資訊安全管理課程教材(96 年 7 月)

11、林秉忠、陳彥銘，無線網路安全白皮書(一)

12、資安人科技網，http://www.informationsecurity.com.tw/

13、臺北縣地政資訊安全政策(95 年 6 月 26 日訂定)

14、臺北縣各地政事務所電腦系統作業程序（範本）(95 年 6 月 26 日訂定)

15、臺北縣各地政事務所資訊儲存媒體安全管理要點(95 年 6 月 26 日訂定)

16、臺北縣網路申領電子謄本試辦作業委外服務案－建議書需求說明書

17、電腦系統異常中斷復原及緊急應變標準作業程序

18、臺北縣政府地政局及各地政事務所資訊發展永續經營計畫(95 年 6 月 26 日訂定)

19、臺北縣各地政事務所電腦系統作業程序(範本)