

臺北縣選舉委員會資通安全管理作業

95.03 初訂

97.02 第 2 次修訂

- 一、目的：臺北縣選舉委員會(以下簡稱本會)為落實資通安全稽核制度,特訂定本作業,規範本會各同仁遵守配合辦理。
- 二、資安稽核時間:每年年底由本會政風室稽核一次為原則,后附資安稽核查核表(附件一)。
- 三、本會資安維護,因涉專業領域及人力限制,以委外方式協助辦理為原則。
- 四、作業項目:
 1. 為確保網路集線櫃及伺服器之安全保護與監督,應設電腦主機房集中管理。
 2. 本會資訊作業環境有重大改變時,應重新進行評估檢討,擬訂保護控制措施。
 3. 有關網路及電子郵件之使用,應利用各種會議管道隨時加強灌輸同仁之使用危機意識,以避免瀏覽惡意網站及遭社交工程攻擊。
 4. 本會各同仁應每季備份自有文件,妥善保管,並每月儲存新還原點,資安管理人員每半年進行回復測試。
 5. 針對主機房進出日誌、資料庫更新存取記錄、審視防火牆及人員存取權限清單等,應定期審查管控,並請主管覆核。
 6. 因本會各項選舉資料至為重要,故本會暫不考慮無線網路之使用。
 7. 本會各同仁應配合本會安全作業管理規範個人使用相關規定(附件二),並每週更新防毒軟體之版本,且不可任意下載非選務所需之軟體,若經發現,稽核人員將逕行回復。
- 五、本作業將隨時配合行政院主計處電子處理資料中心之函示修正補充之。

臺北縣選舉委員會資訊安全作業管理規範

個人使用相關規定

一般保密責任

1. 人員因故離開座位中斷作業時，必須簽退系統或使用畫面鎖定保護，防止帳號被盜用或資料被竊取。
2. 本會同仁應妥善保管個人電腦、磁片、磁帶或隨身碟等儲存媒體，下班或公出離開辦公室前，必須關閉電腦設備並將桌面收拾乾淨。
3. 密等以上之公文及相關資料應上鎖，避免有心人士竊取機密資料或侵入系統。
4. 每部電腦應安裝防毒系統，並隨時啟動防毒監控程式，亦須設定與防毒伺服器主機連線，以定時主動更新病毒碼。
5. 同仁應保持高度之警戒心，防範不法人士以偽裝、騙術獲取帳號及通行碼入侵。並應具備高度之危機意識，如有發現疑似系統安全危機時，應迅速通知本會資通安全人員。

網路系統存取控制

1. 本會同仁利用微軟視窗作業系統之檔案分享功能，提供他人存取檔案時，應僅針對必要對象開放使用權限，避免將權限完全開放。
2. 個人電腦不得安裝或啟用遠端遙控軟體為原則。如有使用需要時，使用者必須經過本會同意後始可安裝及執行遠端遙控軟體，並於使用需求消滅時逕行關閉該項軟體。
3. 網路使用者應恪遵本會之網路安全規定，於授權範圍內存取網路資源，如有違反以下情事，將移送政風室依相關法規查處。
 - (1) 不得以任何方式竊取他人之登入帳號、通行碼。
 - (2) 不得使用任何軟體、設備竊聽網路上之通訊。
 - (3) 不得使用任何手段干擾或妨害網路之正常運作。
 - (4) 不得嘗試入侵防火牆主機。
 - (5) 不得於本會網路上儲存、建置或傳播色情文字、圖片、影像、聲音等資訊。
 - (6) 不得未經核准，私自安裝網路服務或裝置。

電子郵件安全管理規定

1. 本會同仁禁止以電子郵件騷擾他人、發送匿名郵件、偽造他人名義發送郵件或惡意發送大量不當郵件，導致其他網路使用者之不安與

不便。如有違反之情事，由本會政風室查處，必要時由中央選舉委員會資訊室提供技術支援。

2. 密等以上之公文及資料，不得以電子郵件傳遞；敏感性資料如有透過網路傳送之必要，應經加密處理後傳送。
3. 對於來路不明的電子郵件，應通知網路安全管理人員處理，不宜隨意開啟該電子郵件，避免啟動惡意程式，造成本會網路系統遭受感染與破壞。
4. 寄送電子郵件，附件應避免夾帶可執行檔。

通行碼使用與保密責任

1. 使用者須小心保管及使用個人之通行碼，通行碼設定原則如下：
 - (1) 通行碼組成需含英文字母、數字。
 - (2) 通行碼必需為八碼（含）以上。
2. 儘量避免以時間、個人資訊、單位識別代碼、電話號碼或使用者帳號等做為通行碼。
3. 應定期更換通行碼，同一通行碼使用期限最長不得超過六個月，並應儘量避免重複或循環使用舊的通行碼。
4. 個人職務變更時，必須更換通行碼。
5. 個人應負責保護通行碼，維持通行碼的機密性。
6. 應避免將通行碼記錄在書面上，或張貼在個人電腦或終端機螢幕或其他容易洩漏秘密之場所。
7. 當有跡象足以顯示系統及使用者通行碼可能遭破解時，應立即更改通行碼。
8. 第一次登入系統時，應立即更改臨時性通行碼。

個人電腦使用規定

1. 多人使用之個人電腦，使用者不應將個人之帳號與通行碼存放在該公用電腦上，例如：使用瀏覽器上網時，不應記憶該帳號與通行碼。
2. 個人電腦除作業系統本身所預設安裝之軟體、公務用之資訊系統、辦公室軟體、防毒軟體外，使用者不得自行安裝應用軟體。若因公務需要，應向資訊中心提出申請，且該軟體應具有合法之版權。
3. 個人電腦除原本所安裝之資訊硬體零件外，嚴禁私自加裝其它硬體裝置(如網路介面卡、硬碟抽取盒...)。
4. 於個人電腦中所安裝之軟體檔案與相關設定，使用者不得將之移動或刪除，若有問題，應向資訊人員詢問。
5. 本會同仁應使用具有合法版權的軟體，避免交換使用或上網下載來

路不明之軟體、資料。

6. 本會同仁使用由外部交換得來之資料前，應先啟動病毒防護軟體掃描之，若發現異常，應終止使用該資料。
7. 同仁操作電腦系統如發現病毒時應立即清除，並通報資訊人員告知病毒或惡意程式名稱。無法自行清除病毒時通知資訊人員協助處理。

儲存媒體使用規定

1. 使用者應將個人資料儲存於個人電腦 D 磁碟機之儲存空間。
2. 使用者使用磁碟片、外接式儲存媒體（如：隨身碟、硬碟機、燒錄器...）時，應先使用掃毒軟體掃描之，若發現異常，應終止使用該儲存媒體。

臺北縣選舉委員會 年資安稽核查核表

受查單位		受查人員		日期時間	
項次	查核項目說明	查核記錄			
		是	否	說明	
1	是否詳閱並瞭解本會資訊安全政策及資訊安全作業管理規範等相關規定？				
2	帳號密碼強度是否足夠？				
3	個人電腦是否依規定未儲存色情文字、圖片、影像、聲音等資訊？				
4	是否依規定避免將通行碼記錄在書面上，或張貼在個人電腦或終端機螢幕或其他容易洩漏秘密之場所？				
5	是否設定螢幕保護程式，並設有密碼才能開啟？				
6	是否瞭解不應開啟或轉寄來路不明的電子郵件或電子郵件附件之規定？				
7	是否依規定除作業系統預設之軟體、公務用資訊系統、辦公室軟體、防毒軟體外，無自行安裝應用軟體？				
8	是否依規定除原本安裝之資訊硬體零件外，無私自加裝硬體裝置？				
9	是否定期備份個人重要資料？				
10	是否停用檔案或資料夾之分享功能（網路芳鄰）？				
11	郵件收發軟體是否設定停用郵件預覽功能？				
其他說明：					
稽核人員簽章：					