臺北市清江國民小學資訊安全計畫實施要點

壹、依據

臺北市清江國民小學（以下簡稱本校）為推動資訊安全教育，強化資訊安全管理，確保資料、系統、設備及網路安全，保障使用者權益，特依照「行政院及所屬各機關資訊安全管理要點」，訂定本計畫。

貳、目標

1.維持校務行政系統及校園教學網路持續運作。

2.防止駭客、病毒等入侵及破壞校務行政系統及校園網路。

3.防止人為意圖不當及不法使用校務行政系統及校園網路。

4.維護校務行政系統及校園網路實體環境安全。

5.避免人為疏失意外。

6.推廣並實施資訊安全教育，培育具有資訊素養的新一代。

參、實施範圍

一、人員：本校教職員工、學生及使用本校系統資源之委外廠商人員。

二、應用系統：包含教務行政系統、公文系統、校園網路等。

三、硬體設備：

1.行政電腦：校務行政系統所安裝之主機、伺服器及與個人電腦。

2.班級及教師電腦：各班級學生及教師使用之個人電腦。

3.教學電腦(電腦教室)：進行電腦資訊課程所安裝之個人電腦。

四、資訊安全教育：

1.研習活動及宣導：定期舉行資訊安全研習，鼓勵教職員工參加，並利用教師朝會時間，宣導資訊安全，提供新知。

2.班級教學：利用彈性課程，結合資訊議題，設計不同年級所需之資訊安全教育，並實施之。

肆、權責與分工

本校資訊安全工作之權責分工如下：

一、資訊安全政策、計畫及規範之建置及評估等事項，由資訊組負責辦理。

二、資料及資訊系統之安全需求、使用管理及保護等事項，由各業務承辦人員負責辦理。

三、資訊機密維護及資訊安全之稽核事項，由各業務承辦人員辦理。

四、資訊安全教育由本校全體教師共同辦理。

伍、安全管理

一、電腦病毒及惡意軟體之防範

1.伺服器及個人電腦：應有事前預防及保護措施，防制及偵測電腦病毒及惡意軟體等的侵入。

2.電腦病毒防範應考量的重要原則

(1)使用者應遵守軟體授權規定，禁止使用未取得授權的軟體。

(2)使用電腦病毒防制軟體，應依下列原則：

・電腦病毒防治軟體及病毒碼應定期更新版本。

・應定期或即時(real time)掃瞄電腦系統及資料儲存媒體。

・對來路不明及內容不確定的磁片，應在使用前詳加檢查是否感染電腦病毒。

・應定期將必要的資料備份。

二、軟體版權之控管

1、軟體之使用，應遵守相關法令及契約規定。

2、軟體版權管理應考量下列事項：

(1)禁止教職員工及學生保有或使用未取得授權的軟體。

(2)禁止教職員工及學生在未取得授權同意前，將軟體安裝到電腦設備上。

(3)須在原授權許可之外的電腦設備上使用軟體時，應取得正式的授權或另行採購。

(4)應依[政府所屬各級行政機關電腦軟體管理作業要點]規定，建立軟體使用的註冊管理機制。

三、日常作業之安全管理

1.應定期執行必要的資料及軟體備份，以便發生災害或是儲存媒體失效時，可迅速回復正常作業。

2.電腦及網路系統更新、維修、問題處理：

(1)電腦軟硬體及網路系統出現問題時，應迅速報告相關人員或資訊組。

(2)電腦軟硬體及網路系統更新、維修、問題處理應定期記錄，以供日後查考。

四、資料安全之管理

1.電腦媒體之使用管理：

(1)包括可攜帶移動的磁碟、光碟、筆記型電腦等，應依保存規格要求，存放在安全的環境。媒體儲存的資料，不再繼續使用時，應將儲存的內容消除。

(2)內含機密性或敏感性資料的媒體報廢時，應以安全的方式處理，例如：燒毀、以碎紙機處理，或將資料從媒體中完全清除。

(3)資訊累積一段時間作處理時，應特別注意及防止大量非機密性資料彙總成為敏感性或機密性資料。

2.處理、收受機密性、敏感性的資料，應防範洩漏或不法及不當的使用，視各業務單位之需求，可於獨立的或是專屬的電腦中執行，或在傳輸、儲存過程中以加密方法保護

3.個人資料的蒐集、公告、利用、更正、刪除及相關的申請登記、損害賠償、處罰等事宜應依「電腦處理個人資料保護法」等有關法令規定辦理。

4.電子檔案之保管

(1)電子資料檔案應妥善保管定期備份，以防止遺失、損毀、或不當使用。

(2)超過保存時限的檔案，應依相關規定刪除或銷毀。

五、網路安全管理

1.校園網路使用者之管理

(1)本校教職員工及學生，依其身分及所執行之工作，成為合法授權的校園網路使用者（以下簡稱使用者）。

(2)校園網路使用者使用者應遵循以下規定：

・不得將自己的登入身份識別帳號與密碼交付他人使用。

・不得使用他人的登入身份識別帳號與密碼。

・禁止利用校園網路從事不法、不當得利之情事。

・網路使用者不得以任何手段蓄意干擾或妨害校園網路的正常運作。

2.主機之安全防護

(1)避免提供遠端登入，以防資料經由電話線路或網際網路傳送時，被偷窺或截取(如一般網路服務 HTTP、Telnet、FTP 等的登入密碼)。

(2)防制非法使用者假冒合法使用者身分登入主機進行偷竊、破壞等情事。

(3)機密性及敏感性的資料或文件，不得存放在對外開放的資訊系統中。

3.系統之安全管理由資訊組負責，包括伺服主機的開關機，伺服主機的管理，伺服主機的正常運轉，管理者密碼管理，資料的安全管制，資料的備份與復原，網路線路的正常使用。

4.網路入侵之處理

若發現網路被入侵或疑似被入侵時(如：網頁遭竄改、分散式攻擊、資料非法存取、密碼被破解等)，應立即依下列程序處理，並採取必要的行動。

(1)立即拒絕入侵者任何存取動作，防止災害繼續擴大；當防護網被突破時，系統應設定拒絕任何存取；或入侵者已被嚴密監控，在不危害內部網路安全的前題下，得適度允許入侵者存取動作，以利追查入侵者。

(2)切斷入侵者的網路連接，如無法切斷則必須關閉防火牆；或為達到追查入侵者的目的，可考慮讓入侵者做有條件的連接，一旦入侵者危害到內部網路安全，則必須立即切斷入侵者的網路連接。

(3)應全面檢討網路安全措施及修正防火牆的設定，以防範類似的入侵與攻擊。

(4)應正式記錄入侵的情形及評估影響的層面。

(5)立即向權責主管人員報告入侵情形。

(6)事件發生 24 小時內向基隆市教育局的資訊安全緊急處理小組反應通報，以獲取必要的外部協助，並在 72 小時內完成系統修復。

六、網路安全稽核

1.網路安全稽核事項

(1)操作紀錄及作業紀錄應予以保存。

(2)對於通過防火牆之各項連線資訊，均應予記錄。

(3)各伺服主機應記載各項連結服務的作業紀錄(system log)。

2.網路入侵之追查

(1)對入侵者的追查，除使用系統指令執行反向查詢外，並聯合相關單位(如中華電信)，追蹤入侵者。

(2)入侵者之行為若觸犯法律規定，構成犯罪事實，應立即通知有關單位，請其處理入侵者之犯罪事實調查。

七、使用者之註冊及使用理管理

1.對於多人使用的資訊系統(校務行政系統、學校、班級網頁)，必須依循安全的註冊程序。

2.帳號及權限管理，必須考量的事項如下：

(1)確認使用者是否已經取得使用資訊系統之正式授權。

(2)確認使用者被授權的程度是否與業務目的相稱，是否符合資訊安全政策及規定，再依執行業務之需求，賦予使用者系統存取特別權限。

(3)使用者調整職務及離（休）職時，必須儘速註銷其系統存取權限。

(4)確認系統存取特別權限之事項以及人員名單，定期檢查及取消閒置不用的帳號。。

3.密碼之管理

(1)為維持密碼的機密性，使用者須於首次使用時，立即更改通行密碼的方式處理。

(2)使用者忘記通行密碼時，提供臨時的密碼，以利系統辨認使用者。

(3)個人必須負責保護密碼，以維持其機密性。

(4)避免將通行密碼記錄在書面上，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)當有跡象足以顯示系統及使用者密碼可能遭破解時，應立即更改密碼。

(6)密碼的長度最少應由六位長度組成(不得為空白)，且應英數混和。

(7)更換維護廠商時，防火牆及主機之相關帳號及密碼須刪除或修改

八、設備安全管理

1.設備應安置在適當地點，以減少環境不安全引發之危險及未經授權存取系統的機會。

2.設備安置應遵循的原則如下：

(1)設備應儘量安置在不需經常進出之地點。處理機密性資料工作站，應放置在可注意及可就近照顧之地點。

(2)需特別保護之設備，應考量與一般設備區隔。

(3)應檢查及評估火災、煙、水、灰塵、震動、化學效應、電力供應、電磁幅射等加諸於設備之危害。

(4)電腦作業區應禁止抽煙及飲用食物。

(5)應考量其他可能導致之危險因素。

3.辦公桌面之安全管理

(1)公文及磁片長時間不使用及下班後，應妥為存放；機密性、敏感性資訊，應妥為收存。

(2)棄置之手寫或影印公文廢紙及已過保存期限之公文，應視需要予以銷毀。

(3)個人電腦及終端機不使用時，應予關機、登出、設定螢幕密碼或是以其他控制措施保護。

陸、資訊安全事件通報處理機制

一、資訊安全事件之通報

1.因資訊安全事件（包括系統有安全漏洞、遭受非法入侵及破壞、遭遇阻斷服務攻擊及功能不正常事件等），致電腦系統無法運作或影響執行效率時，相關人員應視其狀況嚴重程度及影響層面，循序向各權責主管報告。

2.資訊組發現有資訊安全事件時，應依基隆市資訊小組資訊安全事件通報管道，迅速通報權責主管單位及人員處理。

3.發現資訊安全事件時，應迅速通報資訊組或權責主管單位，或請維護廠商協助處理。

二、通報後應採行之措施

1.應立即停止使用受影響之電腦系統或設備，並保留現況。

2.值班人員接獲通報後應紀錄相關的訊息。

3.系統管理人員處理後，應向直屬業務主管回報處理結果，並作成紀錄。

三、緊急應變計畫

1.人員請假或有緊急事故時，可將重要事項交託職務代理人代為處理，若需人員親自處理時，可透過電話聯繫及網路連線作必要之處置，若家中無電腦之同仁，可以借用筆記型電腦來連線。

2.系統方面緊急應變措施：定期執行資料及軟體之備份及備援作業，以便發生災害或是儲存媒體失效時，可迅速回復正常作業。系統當機時，同仁先自行排除，若無法排除時立即連絡維護廠商處理。

柒、本計畫經校長核可後實施，修正時亦同。