臺東縣利嘉國民小學資訊通訊安全管理要點

96.09.05 初訂
104.09.02 修訂

一、依據 90.12.26 教育部所屬機關及各級公私立學校資通安全工作事項修訂本要點。

二、依據行政院於 94.07.21 核定「政府機關（構）資訊安全責任等級分級作業施行計畫」，本校資訊安全責任等級分級為 D 級，應依其規定辦理維護資訊安全工作。

三、配合「國家資通安全緊急應變中心」建立緊急通報應變組織，建立資訊安全長（副首長以上）及二位資訊安全聯絡人，並列入行政業務交接項目。本校資訊安全長為總務主任，二位資訊安全聯絡人分別為教導主任及資訊教師。

四、發現資安事件或接獲「國家資通安全會報」、相關主管機關通知發生資安事件時，應於規定之應變時限內至「國家資通安全應變網站」進行資安事件通報（https://www.ncert.nat.gov.tw），並於規定時限內處理完成或完成損害控制後至進行結案通報。

五、網路安全管理

（一）應設置防火牆並適當阻絕外部對內之網路連線及通訊埠。

（二）安裝防毒軟體，並適當進行安全檢核。

六、電腦系統安全管理

（一）電腦設備作業系統及相關伺服軟體應適時更新軟體及進行漏洞修補。

（二）電腦設備作業系統應安裝防毒軟體並適時更新病毒資料庫。

（三）作業系統進行遠端維護時，應於加密管道進行，並管制維護來源 IP。

七、應用軟體安全管理

（一）應用程式所有輸入欄位應進行字元檢查，排除不必要特殊字元（如'"!$%^&*_|-><;等）以防止資料庫隱碼攻擊（SQL-injection）。

（二）應用程式進行遠端維護時，應於加密管道進行，並管制維護來源 IP。

八、禁止使用校內電子產品閱覽不當之網路資訊（如暴力、色情、賭博、駭客、惡意網站、釣魚詐欺、傀儡網路等）。

九、禁止於上班時間透過網路資源進行與工作內容無關之串流媒體、MP3、圖片、檔案等網路上的傳輸。

十、非上班時間（中午休息、下班後）的使用，需建立稽核管理機制，不得影響單位內主要系統運作之效率。

十一、非經申請，禁止於上班時間使用即時訊息（Instant Message）、點對點檔案共享（P2P）及 tunnel 相關工具。

十二、不得於網際網路上下載及安裝非經許可之應用程式，以避免資安上的風險（木馬、tunnel 軟體、間諜程式、傀儡程式等）及違反法令之疑慮（著作權、版權）。

十三、上網行為所佔之單位內部頻寬，需以不影響各主系統之網路效能為前提，若有資源上的衝突，將以各主系統為主。

十四、機密文件或不宜公開之檔案文件，非經許可不得透過網際網路工具進行傳輸及檔案交換。

十五、資訊安全管理原則

（一）共通原則

1. 個人電腦應安裝防毒軟體，並經常修補系統漏洞。除定期更新病毒碼與系統漏洞修補程式外，每次開機使用前，建議可以先檢查是否已更新病毒碼及漏洞修補至最新版本。
2. 為避免感染病毒，建議關閉電子郵件預覽窗格功能。
3. 對於來路不明之電子郵件，不宜隨意打開，以免啟動惡意程式執行檔，使個人電腦與資訊系統遭到破壞。
4. 為避免導致他人電腦感染電腦病毒，不任意轉寄來歷不明之電子郵件。
5. 不瀏覽任何可疑或非法網站。
6. 不使用電腦設備時，宜採取登出、設定螢幕保護功能、關機或其他適當之保護措施。
7. 個人電腦應啟用螢幕保護程式功能，並設定密碼保護，於電腦暫時無人使用時可自行啟動。啟動螢幕保護程式的時間設定可依單位或個人之工作業務特性進行調整。
8. 不可運用電子郵件大量傳送廣告信或其他造成收信人困擾之垃圾郵件，避免影響郵件服務系統之正常運作。
9. 傳真機敏或重要之資訊文件時，接收與傳送端皆應確定有人，傳送完成後應立即從傳真機取走。
10. 建立個人資安防護意識，留意資安相關新聞與資訊。

（二）密碼使用原則

1. 避免將帳號、密碼記錄於書面或張貼於容易洩漏之處（例如以便紙書寫個人帳號與密碼貼於電腦螢幕上）。
2. 當發現密碼有可能遭受破解或竊取之可疑跡象時，應立即變更密碼。
3. 於應用軟體完成安裝作業後，應更改該軟體預設之使用者密碼。
4. 使用者一次登入資訊系統時，應更改臨時性啟始（首次使用）密碼。
5. 應設定防禦強度較高之密碼，以下為建議設定原則：
   (1)密碼建議設定至少六碼以上。
   (2)密碼可採用文數字混合、特殊字元符號與大小寫英文字母混合來進行設定。
   (3)密碼沒有明顯意義。

6.不任意向任何人提供個人帳號及密碼。

7.不使用非授權帳號與密碼。

8.宜定期（例如每月、每季、每半年等）變更密碼。

（三）資訊系統管理者或資訊安全管理者

1.資訊系統管理與安全防護

(1)應視資訊系統重要性、系統架構與網路架構選擇適當之安全防護措施（例如防火牆、入侵偵測／防禦系統、防毒軟體等）來提升資安防禦能力。

(2)存放系統使用者申請或註冊的資料檔案，應採用適當授權管控方式或加密方式處理，以防資料外流。

(3)為保護重要檔案及資訊，應採行適當的措施（例如檔案加密、資料備份等），以防止資料遺失、毀壞及被偽造或竄改。

(4)資訊系統應檢測與修補系統漏洞或弱點。於安裝相關修補程式前，建議可先經過評估與測試，以確認不會對系統運作造成負面影響。

(5)資訊系統應盡量避免共用帳號。

(6)系統重要資訊（例如系統紀錄、稽核紀錄等），宜依照單位需求與相關規範來進行備份作業，並應確認備份作業結果之有效性。

(7)宜針對重要資訊系統毀損或失效來制訂相關系統復原計畫與執行步驟。

(8)應確認所管理之系統帳號皆為合法授權者，避免出現閒置帳號或非授權使用者帳號。

(9)定期檢視資訊系統之異常作業相關紀錄，以確認是否有未發現或潛在之資安威脅與弱點。

2.密碼管理

(1)當發現管理者密碼可能遭到破解或竊取之可疑跡象時，應立即變更密碼。

(2)在資訊系統完成安裝作業後，應立即變更該系統預設的管理者密碼。

(3)應定期變更管理者密碼。

十六、本要點經校務會議通過，並陳校長鑑核後實施，修正時亦同。