台南市私立崑山高級中學資訊安全管控計畫

99 年 12 月 20 日行政會報通過實施

壹、 總則

一. 為維護網路資訊系統的正常運作、確保網路資訊傳輸交易安全，並保障本校電腦處理資料之機密性與完整性，特訂定本規範。

二. 參考依據如下：

(一). 「行政院及所屬各機關資訊安全管理要點」第 9 點第 1 項第 3 款規定。

(二). 「政風機構維護公務機密作業要點」第 14 點、第 15 點規定。

(三). 行政院所屬各機關資訊安全管理要點。

(四). 教育部台電字第 0960103352 號函

三. 適用對象：本校教職員工、實習教師、臨時人員與學生等人員。

四. 適用範圍：

(一). 資訊安全政策制定及評估

(二). 人員安全管理及教育訓練。

(三). 電腦系統安全管理。

(四). 系統存取控制。

(五). 需求變更管理。

(六). 資訊資產之安全管理。

(七). 實體及環境安全管理。

(八). 永續運作計劃之管理。

貳、 組織與權責

一. 為統籌本校資訊安全管理事宜，應成立本校「資訊內部稽核管理小組」(以下簡稱資訊小組)，由校長擔任召集人，各科、處室主管負責本校資訊安全管理工作。資訊系統安全控制技術事宜由行政電腦中心負責辦理，資料及資訊系統之安全使用及保護事宜由各處室行政單位負責辦理。必要時，資訊小組得委請校外學者專家提供資訊安全顧問諮詢服務及技術支援協助，並依規定支給相關費用。

二. 資訊小組成員：

(一). 校長

(二). 各科、處室主管

(三). 行政電腦中心

參、 規範內容

一. 資訊安全政策的制定及評估

(一). 資訊安全政策之制定：資訊安全政策的目的為防禦一切有計畫的、意外的、來自內部的或外部的威脅，以保護本校資訊資產的安全。為表達本校對資訊安全推動之支持與決心，應制定資訊安全政策。

(二). 資訊安全政策與管理規範之評估：資訊安全政策、管理規範及相關管理辦法應每年定期進行獨立及客觀的評估，以反映資訊安全管理政策、法令、技術及單位業務之最新狀況，確保資訊安全實務作業之可行性及有效性。

二. 人員安全管理及教育訓練

(一). 人員安全管理：

1. 本校各委外開發維護之廠商人員，必須簽署保密協定及切結遵守本資訊安全管理規範之規範。
2. 網路使用者如因職務異動而成為非授權使用者時，相關單位應主動通知網路系統管理人員撤銷該使用者帳號。

(二). 人員教育訓練：

1. 各處室對該單位新進人員應施以適當的系統操作訓練，避免使用者不當之操作。
2. 新系統上線時，應對其作業人員、維護人員及網路管理人員施以適當的教育訓練。
3. 每年度應對校內同仁辦理資訊安全管理課程宣導或訓練，提升其危機意識與資訊安全觀念。課程中必須給予完整之軟體著作權與版權觀念，嚴禁非法使用軟體，而自由軟體(freeware)與共享軟體(shareware)之安裝使用亦必須詳細了解其版權宣告並遵守。
4. 每年度應針對校內資訊從業人員辦理資訊安全管理及危機處理防護課程訓練。
5. 應隨時注意資通安全最新訊息，參與資通安全相關訓練，並利用內部網站公告同仁知悉

三. 電腦系統安全管理

(一). 電腦病毒及惡意軟體之防範：

1. 本校同仁應使用具合法版權軟體，避免上網下載來路不明之軟體。
2. 與外部交換資料時，使用資料前應啟動病毒防護軟體偵測。
3. 同仁應隨時更新病毒碼並下載修補系統漏洞。
4. 同仁操作電腦系統如發現病毒時應立即清除，並通報資訊小組病毒或惡意程式名稱。無法自行清除病毒時通知資訊小組協助處理。

(二). 作業權限與帳號管理：

1. 核發使用者帳號、密碼前，應查核使用者是否已取得使用資訊系統之正式授權，及其授權之程度是否與業務目的相對稱。在未完成正

式授權前，不得對該使用者提供存取服務。

2. 使用者帳號名稱不應帶有足以辨識使用者權限的資訊。
3. 應嚴格管控應用系統之特別權限，視個別執行業務之需求，逐項考量賦予使用者系統特別權限之存取。
4. 應用系統設計使用者帳號、密碼時應遵循安全原則

(三). 個人隱私之保護

1. 資訊系統處理個人隱私資料時，審慎處理個人資料，非公務用途嚴禁調閱使用。
2. 提供公眾服務的資訊系統，如有存放民眾申請或註冊之私人資訊，應將資訊獨立於系統之外，避免有心人士竊取，侵犯民眾隱私。
3. 個人資料依有關法令為特定目的外之利用時，應由該資料檔案承辦單位簽奉核准後行之。

(四). 系統登入安全管理

1. 系統登入程序應於使用者完成所有登入資料輸入後，始開始查驗登入資訊的正確性，登入失敗時，系統不應提供訊息告知使用者錯誤之資料項目。
2. 系統登入失敗次數應以三次為限，並應紀錄此登入失敗事件後中斷連線，並強制該終端個人電腦必須間隔一段時間後才能再嘗試登入。

(五). 資訊安全事件通報處理程序

1. 應建立處理資訊安全事件之作業程序，並課予相關人員必要的責任，以便迅速有效處理資訊安全事件。
2. 資訊安全事件處理程序，至少應含括電腦當機及中斷服務、業務資料不完整或資料不正確導致的作業錯誤、及機密性資料外洩。
3. 應以審慎及正式的行政程序，處理資訊安全及電腦當機事件。權責單位主管遇資訊安全事件時，立刻通知資訊小組。

四. 系統存取控制

(一). 機密性／敏感性系統之作業管控

1. 對機密或敏感性的系統，宜建置獨立的或專屬的電腦作業環境。
2. 應用系統是否屬於機密或敏感性應由系統負責單位決定。
3. 機密或敏感性的應用系統須分享相關資源時，應經系統負責單位主管核可。

(二). 使用者存取管理：

1. 本校新進人員及委外服務人員由資訊小組核發帳號後，啟用電腦系統。帳號及通行碼嚴格禁止交付他人，職務代理時須建立代理帳號，亦不可於電話中告知系統維護人員。
2. 所有網路使用者僅核發一個使用者帳號，如有特殊情形（如系統測試、免費軟體下載等用途），經會簽資訊小組並奉核定後，始得核

發匿名或多人共享的帳號。

3. 應用系統維護人員應定期檢討及評估相關使用者之存取權限。
4. 為防止有人未經正式的授權程序取得特別權限，應定期檢討系統存取特別權限之核發情形。

(三). 系統存取之責任：

1. 人員因故離開座位中斷作業時，必須關閉系統或使用畫面鎖定保護，防止帳號被盜用或資料被竊取。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，避免有心人士竊取機密資料或侵入系統。
2. 同仁應保持高度之警戒心，防範不法人士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，應迅速通知資訊小組。

(四). 網路系統之存取控制：網路使用者應遵守本校之網路安全規定，於授權範圍內存取網路資源，不得以任何方式竊取他人之登入帳號、密碼，不得使用任何手段干擾或妨害網路之正常運作，不得嘗試入侵防火牆主機，亦不得於本校網路上儲存、建置或傳播色情文字、圖片、影像、聲音等資訊。如有違反以上情事，移送資訊小組依相關法規查處。

五. 需求變更管理

(一). 資訊小組每年視狀況辦理資訊系統之更新作業。

(二). 因應臨時業務需求，需求單位應由業務單位填寫向承辦人員申請，承辦人員得視人力、技術及成本考量，提出可行性方案及意見（或辦理情形）回覆原需求單位。

六. 資訊資產之安全管理

(一). 資訊設備安全管理

1. 本校各項資訊設備除依照相關審計法規財產管理外，各單位應自行負責設備之安全，移出本校時應經權責單位主管核定始得放行。
2. 本校各項資訊設備報廢時，除依相關財產減損規定辦理外，應經秘書檢查其堪用狀況後始得辦理報廢。
3. 本校同仁如發現有不明人士，未經許可擅接網路之情事，應立即通知資訊小組處理，以掌握本校整體資訊設備之安全。

(二). 機密或敏感資訊之安全管理：機密性或敏感性的資料，不得存放於對外開放的資訊系統中。

七. 實體及環境安全管理

(一). 實體設備及環境之安全管理

1. 電腦主機系統及其相關儲存與網路連結設備必須使用穩壓與不斷

電(Uninterruptible Power Supply：UPS)系統供應電力，以避免電壓不穩定或瞬間斷電造成損害。

2. 如發現有不明人士，未經許可擅接網路之情事，應立即通知資訊小組處理，以掌握本校整體資訊設備之安全。
3. 電腦設備之搬遷必須經過資訊小組同意與授權，被授權之搬遷人員必須負責遷移設備之使用安全與內存系統資料安全。

(二). 媒體、文件安全管理

1. 涉及機密性或敏感性之相關媒體、文件由業務單位指定專人保管。
2. 系統文件應妥善保管。如係委外操作之系統，應於合約規範於契約解除時歸還本校。

八. 永續運作計畫之管理

(一). 保全處理程序

1. 發現網路入侵之處理步驟：
   網路使用者發現網路入侵之情事時應立即通知資訊小組，以防止災害繼續擴大。
2. 資訊小組應全面檢討網路安全措施及修正防火牆的設定，尋求適當之解決辦法，以防禦類似的入侵與攻擊。

(二). 突發事件應變辦法

任何突發之安全事件或造成運作中斷之事件，本校同仁不得隨意接受新聞媒體採訪發言，須經校內分析整理後統一發言

肆、 實施時間

一. 自即日起，每半年(6、12 月)由各處室、各科自行執行「資訊內部稽核」1次，並填寫「台南市私立崑山高級中學資訊內部稽核檢查表」(見附件一)，交至資訊小組。

二. 資訊小組得以不定期突擊稽核本校所有單位。

伍、 附則

一. 本規範未訂定之事項，悉依行政院所頒訂之「行政院所屬各機關資訊安全管理規範」及現行法令、規定及教育部相關作業規範相關規定辦理。

二. 本規範經行政會議通過後實施，修正時亦同。

附件一

台南市私立崑山高級中學資訊內部稽核檢查表

查核單位：

查核人員：　　查核日期：　　年　　月　　日

查　核　事　項	查　核　結　果		
	是	否	說明
一、資訊內部稽核編組			
1.有無配合電腦中心人員進行不定期內部稽核？			
2.內部人員違反規定，是否建立單位主管通報管道？			
二、系統存取權限（帳號）管理			
1.自行下載安裝非法軟體、音樂檔、電影檔之類的多媒體檔案？			
2.將公務及學生資料外傳給非相關人員?			
3.電腦借給學生或校外人士使用？			
4.下班後電腦沒有關機？			
三、密碼複雜度管理情形			
1.登入電腦系統畫面是否有密碼？			
2.校務行政密碼是否有定期更換？			
四、資料防護			
1.電腦是否安裝防毒軟體？			
2.是否定期備份重要檔案及資料？			
五、其他有關資訊安全事項			
受檢單位人員：			