國立嘉義高中資通安全管理要點

中 華 民 國 100 年 3 月 30 日

一、目標

本要點為規定嘉義高中（以下簡稱本校）資通安全管理作業實施方式，以增進資訊作業之安全性，確保學校資料之機密性、完整性與可用性。

二、目標適用範圍

本校電腦、資訊與網路服務相關的系統、設備、程序、及人員。

三、實施規定

1. 網路安全

1.1 網路控制措施

- 本校與外界連線，應僅限於經由本校網路機房及嘉義市教育網路中心之管控，以符合一致性與單一性之安全要求。
- 應禁止以電話線連結主機電腦或網路設備。

1.2 服務委外廠商合約之安全要求

- 各單位辦理資訊業務委外或硬體維護委外時，應於研議階段提出資訊安全需求，明訂廠商之資訊安全責任及保密規定，並列入契約中，明訂罰則，並要求廠商必須簽訂安全保密切結書（切結書格式參見文件編號 A-1）。

2. 系統安全

2.1 職責區隔

- 本校伺服器主機可依個別應用系統之需要，設置專屬電腦，例如網路服務主機（DNS、電子郵件、網站主機）、教學系統主機、校務基金系統、學籍資料系統主機等。
- 本校的行政系統主機（例如人事、公文、校務基金系統、財產管理系統、薪資管理系統、健康資訊系統、學籍成績資料系統、社團德行系統、圖書管理系統等），由建置處室自行統籌、管理與維護。

2.2 對抗惡意軟體、隱密通道及特洛依木馬程式

- 本校內的個人電腦應：

- 未安裝自動還原功能之電腦皆應裝置防毒軟體，並將防毒軟體設定為自動定期更新病毒碼；或由伺服器端進行病毒碼更新的管理。
- 電腦使用人應自行定期（至少每個月）進行如「Windows Update」之程式更新作業，以防範作業系統之漏洞。
- 應啟動 Windows 內建個人防火牆功能，避免他人非法入侵之風險。

- 本校內個人電腦所使用的軟體應有授權。
- 新伺服器系統啟用前，應經過掃毒與更新系統密碼程序，以防範可能隱藏的病毒或後門程式。

2.3 資料備份

- 各系統管理人員需針對其所管理的重要系統（例如系統檔案、網站、資料庫等）定期進行備份工作或採用自動備份機制；週期為每週至少進行一次。
- 一般行政人員亦應自行定期實施資料備份，以免因中毒或硬碟損毀造成業務資料損失。
- 所有電腦使用者，應避免將個人重要業務資料置於系統磁碟（C：）或 Windows 桌面，以免因中毒或系統重灌造成業務資料損失。

2.4 操作員日誌

- 本校各系統管理人員需針對重要的電腦系統進行檢查、維護、更新等動作時，應針對這些活動填寫日誌予以紀錄，作為未來需要時之檢查。（操作日誌文件參見文件編號 A-2）

2.5 資訊存取限制

- 本校內所共用的個人電腦應以特定功能為目的，並設定特定安全管控機制（例如限制從網路非法下載檔案行為、限制自行安裝軟體行為、限制特定資料的存取、禁止操作線上遊戲等）。

2.6 使用者註冊

- 本校應制定主機系統使用的使用者註冊及註銷程序，透過該註冊及註銷程序來控制使用者資訊服務的存取，該作業應包括以下內容：
  - 使用唯一的使用者識別碼（ID）。
  - 檢查使用者是否經過系統管理單位之授權使用資訊系統或服務。
  - 保存一份包含所有識別碼註冊的記錄。
  - 使用者調職或離職後，應移除其識別碼的存取權限。
  - 每學期檢查並取消多餘的使用者識別碼和帳號。
  - 每學期檢查新增之帳號，若有莫名帳號產生，應關閉帳號權限。

2.7 特權管理

- 本校的電腦與網路系統資訊具有存取特權人員清單、及其所持有的權限說明，應予以文件化記錄備查。

2.8 通行碼之使用

- 管制使用者第一次登入系統時，必須立即更改預設通行碼，預設通行碼應設定有效期限。
- 資訊系統與服務應避免使用共同帳號及通行碼。
- 由學校發佈通行碼（Password）制定與使用規則給使用者（優質通行碼設定原則與使用原則，參見文件編號 A-3），內容應包含以下各項：
  - 使用者應該對其個人所持有通行碼盡到保密責任。
  - 要求使用者的通行碼設定，避免使用易於猜測之數字或文字，例如生日、名字、鍵盤上聯繫的字母與數字（如 12345678 或 asdfghjk），以及過多的重複字元等。或建議通行碼應該包含英文字大小寫、數字、特殊符號等四種設定中的三種。
- 因特殊需要擁有多個帳號時，可考慮使用一組複雜但相同的通行碼。

2.9 通報資訊安全事件與處理

- 資訊安全事件包括：任何來自網路的駭客攻擊、植入木馬程式、病毒感染、垃圾郵件、資料或網頁遭竄改、以及通訊中斷等。
- 學校需建立資訊安全事件通報程序（參見文件編號 A-4）以及資通安全事件通報單（參見文件編號 A-5）；通報程序應包括學校內部通報、學校與所屬縣市教育網路中心的通報、以及教育機構資安通報平台網路通報。
- 當學校內部無法處理之資通安全事件，應通報其所屬縣市網路中心。
- 所訂出資訊安全事件通報程序應公布於校園內使用電腦與網路之場所，提供使用者瞭解。
- 資通安全事件處理完畢後，需填寫資通安全事件解除通報單（參見文件編號 A-6）後，方能解除列管。
- 資訊安全事件等級，由輕微至嚴重區分等級如下：
  - 0 級：教育部及嘉義市教育網路中心檢舉信箱通告之資安事件。
  - 符合下列任一情形者，屬 1 級事件：
    - ☐ 非核心業務資料遭洩漏。
    - ☐ 非核心業務系統或資料遭竄改。
    - ☐ 非核心業務運作遭影響或短暫停頓。
  - 符合下列任一情形者，屬 2 級事件：
    - ☐ 非屬密級或敏感之核心業務資料遭洩漏。
    - ☐ 核心業務系統或資料遭輕微竄改。
    - ☐ 核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。

- 符合下列任一情形者，屬 3 級事件：
  - ☐ 密級或敏感公務資料遭洩漏。
  - ☐ 核心業務系統或資料遭嚴重竄改。
  - ☐ 核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。
- 符合下列任一情形者，屬 4 級事件：
  - ☐ 國家機密資料遭洩漏。
  - ☐ 國家重要資訊基礎建設系統或資料遭竄改。
  - ☐ 國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

- 本校任何人於校內發現異常情況或疑似資安事件及應立即向資訊教師（組長）通報，並填寫「資通安全事件通報單」，資訊教師（組長）應儘速進行處理並研判事件等級。
- 資訊教師（組長）當發生研判事件等級 3（含）以上之事件，應立即通報資訊業務主管及本校校長，並以電話聯絡嘉義市教育網路中心資安承辦人，由校長儘快召集會議研商處理的方式。
- 當本校發生內部無法處理之資通安全事件，應通報嘉義市教育網路中心協助處理。
- 資安事件若需對外通報，由資訊教師(組長)登入教育機構資安通報平台填報。

3. 實體安全

3.1 設備安置及保護

- 本校重要的資訊設備（如主機機房）應置於設有空調空間。
- 本校資訊設備主機機房及電腦教室區域，應設置滅火設備，並禁止擺放易燃物或飲食。
- 本校資訊設備主機機房及電腦教室區域內的電源線插頭應有接地的連結或有避雷針等裝置，避免如雷擊事件所造成損害情況。
- 本校資訊設備主機機房及電腦教室區域，應於出入口處設置門禁的機制。

3.2 電源供應

- 本校重要的資訊設備（如主機機房）應有適當的電力設施，例如設置 UPS、電源保護措施，以免斷電或過負載而造成損失。

3.3 纜線安全

- 本校資訊設備主機機房及電腦教室區域內網路線應建佈於高架地板或需有保護設施。

3.4 設備與儲存媒體之安全報廢或再使用

- 所有包括儲存媒體的設備項目，在報廢前應先確保已將任何敏感資料和授權軟體刪除或覆寫。

3.5 設備維護

- 與校園資訊安全有關之軟硬體設備，應定期與設備廠商建立維護合約。
- 廠商進入機房前需先確認已簽訂安全保密切結書。
- 廠商不可在無任何管理人員陪同之情況下,自行進入主機機房等安全管制區域。
- 校內設備維修應由廠商到場維修為原則，如需將設備攜出校園外，需先將設備之儲存裝置（如硬碟、隨身硬碟、USB 隨身碟、磁帶、光碟片等）先行移除，交由本校使用者自行妥善保管，廠商方得攜出維修。如為儲存裝置損壞需將設備攜出維修，廠商需先簽訂安全保密切結書，使得攜出校園。

3.6 財產攜出

- 未經授權不應將學校的資訊設備、資訊或軟體攜出所在地。但若與執行與業務相關工作者除外。
- 當有必要將設備移出，應檢視相關授權，並實施登記與歸還記錄。

3.7 桌面淨空與螢幕淨空政策

- 結束工作時，所有學校教職員工應將其所經辦或使用具有機密或敏感特性的資料（如公文、學籍資料等）及資料的儲存媒體（如 USB 隨身碟、隨身硬碟、磁碟片、光碟等）妥善存放。
- 本校提供教職員工或學生使用的個人電腦應設定保護裝置，如個人密碼以及螢幕保護。公用電腦則不在此限。

4. 人員安全

4.1 將安全列入工作執掌中

- 應將資訊安全責任納入教職員相關規範，以強化工作上之資訊安全意識。
- 因業務需要將機敏資料交付委外廠商時（如辦理保險、校外教學、畢業紀念冊製作等），廠商必須簽訂安全保密切結書。

4.2 資訊安全教育與訓練

- 本校各系統管理人員應有足夠能力執行日常基礎之資安管理系統維護工作，並使其瞭解資安事件通報之程序。
- 本校鼓勵資訊老師/組長/系統管理人員以及所有教職員參與資訊安全教育訓練或宣導活動，以提昇資訊安全認知。

5. 應對以下各項相關法令有基礎之認知

5.1 智慧財產權

- 著作權法
- 經濟部智慧財產局

5.2 個人資訊的資料保護及隱私

- 電腦處理個人資料保護法
- 個人資料保護法

5.3 電子簽章法

- 電子簽章法
- 電子簽章法施行細則
- 核可憑證機構名單

五、本規範經校長核定後實施，修正時亦同。

文件編號：A-1

資訊軟硬體服務委外單位服務暨保密切結書

_____公司(以下簡稱為本公司)為配合 **國立嘉義高級中學**（以下簡稱為貴校）之資訊應用業務需求，進行相關資訊系統或軟體開發、測試、建置及維護等工作。本公司提供服務項目如下：

一、

二、

三、

四、

五、

(註：列出貴公司將會提供之服務項目)

本公司願意在對貴校提供上述服務項目範圍內之服務時，保證因提供業務服務需存取貴校資料，凡屬與公務機密、個人及事業單位權益相關之資料，無論其內容之一部或全部，均負保密之責；相關資料均以留在貴校內部範疇內處理，倘須由本公司攜至校外處理，應簽奉貴校核可。

本公司亦不私自蒐集貴校所擁有之任何資訊。若所提供之業務服務，不符合上述之規定或經營之服務項目超出上述範圍，或違犯法令，本公司同意無異議接受接受法律制裁與及其訴訟費用，並負責所引發之各項損失賠償。此致

國立嘉義高級中學

申請單位及負責人蓋章：

日期：　　年　　月　　日

本服務暨保密切結書一式兩份，分別由_____公司以及 國立嘉義高級中學 保存

文件編號：A-2

操作日誌

填寫日期：　　民國＿＿＿＿年＿＿＿＿月＿＿＿＿日

系統操作起始時間：　＿＿＿＿時＿＿＿＿分

系統操作結束時間：　＿＿＿＿時＿＿＿＿分

操作事項	□ 系統例行檢查 □ 系統維護 □ 系統更新操作
操作設備對象	
系統錯誤說明	
採取改正措施說明	

操作人員：＿＿＿＿＿＿＿＿　　簽名欄：＿＿＿＿＿＿＿＿

日誌記錄人員：＿＿＿＿＿＿＿＿　　簽名欄：＿＿＿＿＿＿＿＿

文件編號：A-3

優質通行碼設定原則與使用原則

一、 良好的通行碼設定原則

1. 混合大寫與小寫字母、數字，特殊符號。
2. 通行碼越長越好，最短也應該在 8 個字以上。
3. 至少每三個月改一次密碼。
4. 使用技巧記住通行碼
   - 使用字首字尾記憶法：
     a. My favorite student is named Sophie Chen，取字頭成為 mFSinsC
     b. There are 26 lovely kids in my English class，取字尾成為 Ee6ysnMEc
   - 中文輸入按鍵記憶法：
     a. 例如「通行碼」的注音輸入為「wj/ vu/6a83」

二、 應該避免的作法

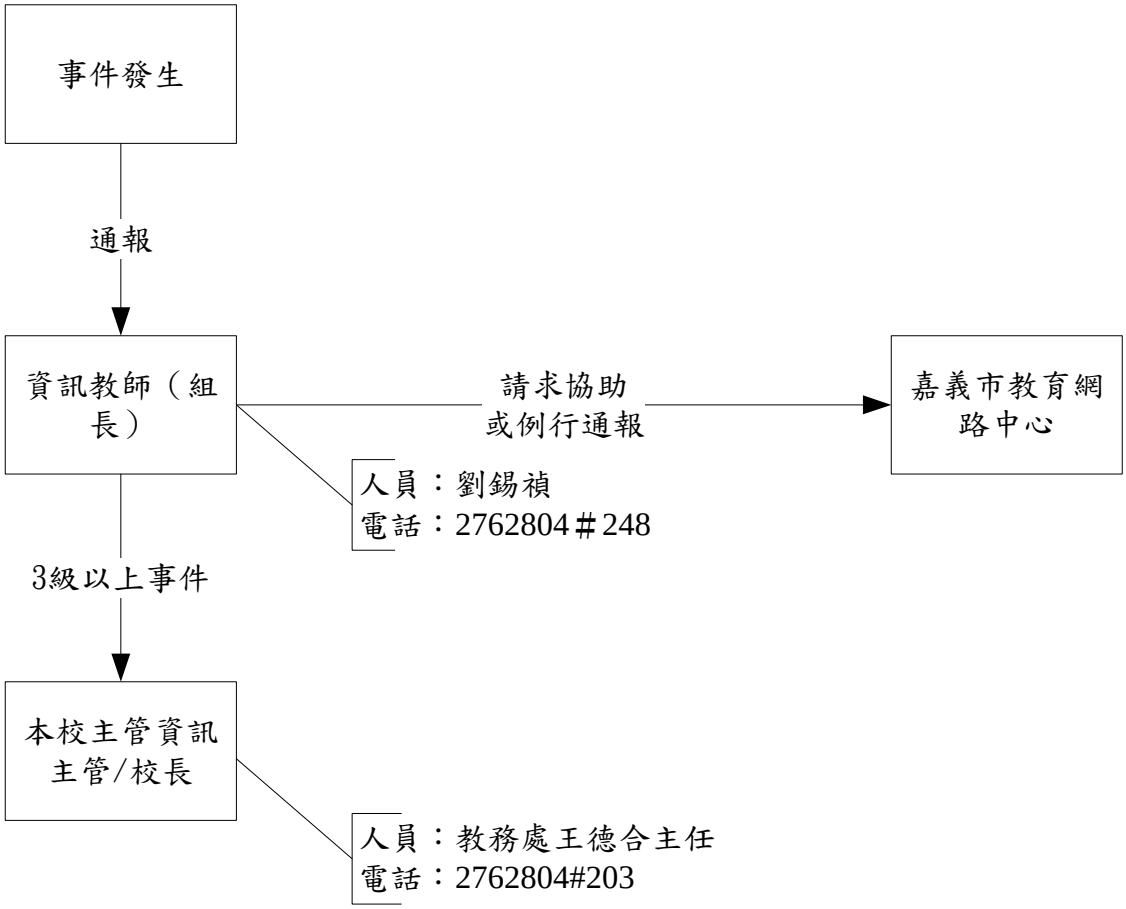
1. 嚴禁不設通行碼
2. 通行碼嚴禁與帳號相同
3. 通行碼嚴禁與主機名稱相同
4. 不要使用與自己有關的資訊，例如學校或家裡電話、親朋好友姓名、身份證號碼、生日等。
5. 不重覆電腦鍵盤上的字母，例如 6666rrrr 或 qwertyui 或 zxcvbnm。
6. 不使用連續或簡單的組合的字母或數字，例如 abcdefgh 或 12345678 或 24681024
7. 避免全部使用數字，例如 52526565
8. 不使用難記以至必須寫下來的通行碼。
9. 避免使用字典找得到的英文單字或詞語，如 TomCruz 、superman
10. 不要使用電腦的登入畫面上任何出現的字。
11. 不分享通行碼內容給任何人，包括男女朋友、職務代理人、上司等。

延伸參考：

"Password Management Guideline", by department of defense computer security center, 12 April 1985 http://www.radium.ncsc.mil/tpep/library/rainbow/CSC-STD-002-85.pdf

文件編號：A-4

資通安全事件通報程序



文件編號：A-5

國立嘉義高中資通安全事件通報單

填報時間：＿＿＿年＿＿＿月＿＿＿日＿＿＿時＿＿＿分　　編號：＿＿＿＿＿＿＿＿

一、 發生資通安全之處室聯絡資料：

處室名稱：＿＿＿＿＿＿＿＿　E-MAIL：＿＿＿＿＿＿＿＿＿＿＿＿

聯絡人：＿＿＿＿＿＿　職稱：＿＿＿＿＿＿　電話：＿＿＿＿＿＿　傳真：＿＿＿＿＿＿

二、 資通安全事件通報事項：

1. 事件發生時間：＿＿＿年＿＿＿月＿＿＿日＿＿＿時＿＿＿分

2. 電腦主機（或伺服器）資料：

◎ IP 位址（IP Address）:＿＿＿＿＿＿＿＿＿＿＿＿

◎ 網際網路資訊位址（Web URL）:＿＿＿＿＿＿＿＿＿＿＿＿（若無，則免填）

◎ 設備廠牌、機型：＿＿＿＿＿＿＿＿＿＿＿＿

◎ 作業系統名稱、版本：＿＿＿＿＿＿＿＿＿＿＿＿

◎ 受駭應用軟體名稱、版本：＿＿＿＿＿＿＿＿＿＿＿＿（若不清楚，則免填）

◎ 已裝置之安全機制：＿＿＿＿＿＿＿＿＿＿＿＿

◎ 其他：＿＿＿＿＿＿＿＿＿＿＿＿

3. 資通安全事件分類：

◎ 事件分類：□非法入侵 □感染病毒 □阻斷服務 □其他：＿＿＿＿＿＿＿＿

◎ 破壞程度：□系統當機 □資料庫毀損 □網頁遭竄改 □其他：＿＿＿＿＿＿＿＿

◎ 事件說明：（文字勿超過 200 中文字）

4. 資通安全事件資料：

影響等級：綜合評估等級取機密性衝擊、完整性衝擊、可用性衝擊最大值

（1）機密性衝擊：【單選】

□ 1 級-非核心業務資料遭洩漏。

□ 2 級-非屬密級或敏感之核心業務資料遭洩漏。

□ 3 級-密級或敏感公務資料遭洩漏。

□ 4 級-國家機密遭洩漏。

（2）完整性衝擊：【單選】

□ 1 級-非核心業務系統或資料遭竄改。

□ 2 級-核心業務系統或資料遭輕微竄改。

□ 3 級-核心業務系統或資料遭嚴重竄改。

□ 4 級-國家重要資訊基礎建設系統或資料遭竄改。

（3）可用性衝擊：【單選】

□ 1 級-非核心業務遭影響或短暫停頓。

□ 2 級-核心業務遭影響或系統停頓，於可容忍中斷時間內回復正常。

□ 3 級-核心業務遭影響或系統停頓，無法於容忍中斷時間內回復正常。

□ 4 級-國家重要資訊基礎建設運作遭影響或系統停頓，無法於容忍中斷時間內回復正常。

◎ 可能的影響範圍及損失評估：（文字勿超過 200 中文字）

◎ 採取的緊急應變措施：

承辦人簽章：	單位主管簽章：

備註：如發現或懷疑有重大資安事件時，請先電話連繫網管老師(分機 248)，並填寫本通報單，簽章後交給網管老師。

文件編號：A-6

國立嘉義高中資通安全事件解除通報單

填報時間：＿＿＿年＿＿＿月＿＿＿日＿＿＿時＿＿＿分　　編號：＿＿＿＿＿＿

一、 發生資通安全之處室聯絡資料：

處室名稱：＿＿＿＿＿＿＿＿　E-MAIL：＿＿＿＿＿＿＿＿＿＿＿＿

聯絡人：＿＿＿＿＿＿　職稱：＿＿＿＿＿＿　電話：＿＿＿＿＿＿　傳真：＿＿＿＿＿＿

二、 資通安全事件通報事項：

1. 事件發生時間：＿＿＿年＿＿＿月＿＿＿日＿＿＿時＿＿＿分

2. 電腦主機（或伺服器）資料：

◎ IP 位址（IP Address）:＿＿＿＿＿＿＿＿＿＿＿＿

◎ 網際網路資訊位址（Web URL）:＿＿＿＿＿＿＿＿＿＿＿＿（若無，則免填）

◎ 設備廠牌、機型：＿＿＿＿＿＿＿＿＿＿＿＿

◎ 作業系統名稱、版本：＿＿＿＿＿＿＿＿＿＿＿＿

◎ 受駭應用軟體名稱、版本：＿＿＿＿＿＿＿＿＿＿＿＿（若不清楚，則免填）

◎ 已裝置之安全機制：＿＿＿＿＿＿＿＿＿＿＿＿

◎ 其他：＿＿＿＿＿＿＿＿＿＿＿＿

3. 資通安全事件分類：

◎ 事件分類：□非法入侵 □感染病毒 □阻斷服務 □其他：＿＿＿＿＿＿

◎ 破壞程度：□系統當機 □資料庫毀損 □網頁遭竄改 □其他：＿＿＿＿＿＿

◎ 事件說明：（文字勿超過 200 中文字）

4. 資通安全事件資料：

影響等級：綜合評估等級取機密性衝擊、完整性衝擊、可用性衝擊最大值

（1）機密性衝擊：【單選】

□ 1 級-非核心業務資料遭洩漏。

□ 2 級-非屬密級或敏感之核心業務資料遭洩漏。

□ 3 級-密級或敏感公務資料遭洩漏。

□ 4 級-國家機密遭洩漏。

（2）完整性衝擊：【單選】

□ 1 級-非核心業務系統或資料遭竄改。

□ 2 級-核心業務系統或資料遭輕微竄改。

□ 3 級-核心業務系統或資料遭嚴重竄改。

□ 4 級-國家重要資訊基礎建設系統或資料遭竄改。

（3）可用性衝擊：【單選】

□ 1 級-非核心業務遭影響或短暫停頓。

□ 2 級-核心業務遭影響或系統停頓，於可容忍中斷時間內回復正常。

□ 3 級-核心業務遭影響或系統停頓，無法於容忍中斷時間內回復正常。

□ 4 級-國家重要資訊基礎建設運作遭影響或系統停頓，無法於容忍中斷時間內回復正常。

◎ 影響範圍及損失評估：（文字勿超過 200 中文字）

三、 解決辦法：

四、 已解決時間：＿＿＿年＿＿＿月＿＿＿日＿＿＿時＿＿＿分；敬請　解除列管。

承辦人簽章：	單位主管簽章：

備註：資通安全事件處理完畢時，請連繫網管老師，並填寫本通報單；本通報單並將通報教育機構資安通報平台。。