稻香國小

資通安全管理規範

中 華 民 國 105 年 11 月 30 日

## 一、 目標

本文件提供國中、小學資通安全系統管理實施原則建議，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、 適用範圍

國中、小學內電腦、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

1.1.1 與外界連線，應僅限於經由教育局(處)網路管理單位之管控，以 符合一致性與單一性之安全要求。

1.1.2 應禁止以私人架設網路（如：電話線、2G 或 3G 網路等）連結機 房內之主機電腦或網路設備。

1.1.3 宜依業務性質之不同，區分不同內部網路網段，例如：教學、行 政、宿網等，以降低未經授權存取之風險。

1.1.4 對於開放提供外部使用者或廠商存取之服務，必須限制使用者之

來源 IP 及網路連線埠(Port)，以確保安全。

1.2 無線網路存取

1.2.1 應禁止使用者私自將無線網路存取設備介接至校園網路；若有介 接之必要應經權責管理人員同意並設定帳號通行碼或加密金鑰 以防未經許可之盜用。

1.2.2 校園內應提供無線網路存取服務，並採取適當安全管控措施：

 專供行政使用之無線網路熱點建議設定加密金鑰防護，並避免 使用開放之無線網路存取重要資訊系統及處理敏感性資料。

 於教學區域、會議室等場所佈建之無線網路熱點應具有使用者

身分認證機制，並經由校園無線路漫遊服務系統提供外校來 賓使用。

 專供師生教學活動使用之無線網路熱點，若採用其他管理方式 確有不便時，應採取限定開放時間及限制開放區域等管理措 施，減少遭受不當利用之機會。

 開放校外人士出入之公共空間可視需要提供民眾無線上網服 務，其網段應與校園網路隔離，或委由網路服務業者提供。

2 系統安全

2.1 設備區隔

伺服器主機可依個別應用系統之需要，設置專屬主機，以避免未經授權 之存取，例如網路服務主機(電子郵件、網站主機)、教學系統主機(例 如隨選視訊主機)等。

2.2 對抗惡意軟體、隱密通道及特洛依木馬程式

2.2.1 個人電腦應：

 裝置防毒軟體，將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。

 作業系統及軟體應定期更新，以防範系統漏洞。 2.2.2 個人電腦所使用的軟體應有授權。

2.2.3 新伺服器系統啟用前，應執行相關程序(如：確認適合該作業系 統之掃毒工具、預設通行碼更新、系統更新等，並記錄於啟用與 報廢紀錄單)，以防範可能隱藏的病毒或後門程式。（參考啟用與 報廢紀錄單格式，文件編號 A-1）

2.3 桌面淨空與螢幕淨空政策

2.3.1 個人電腦辦公桌面應避免存放機敏性文件，結束工作時，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） 妥善存放。

2.3.2 當個人電腦或終端機不使用時，應使用鍵盤鎖或其他控管措施保 護個人電腦及終端機安全個人電腦應設定螢幕保護機制。

2.4 資料備份

2.4.1 系統管理人員需針對學校重要電腦系統及資料（如:系統檔案、 網站、資料庫等）應每週至少進行一次備份工作；建議使用設備

執行異地備份或使用光碟、隨身碟或外接式硬碟執行異地存放。 2.4.2 每年應定期檢查備份資料之可用性與完整性。

2.5 資訊工作日誌

2.5.1 系統管理人員需針對重要電腦系統進行檢查、維護、更新等動作 時，應針對這些活動填寫日誌予以紀錄，作為未來需要時之查 核。（參考資訊工作日誌格式，文件編號 A-2）

2.5.2 系統管理人員應至少每季執行一次校時。

2.6 資訊存取限制 共用的個人電腦（如：電腦教室電腦、教師休息室電腦等）應以特定功 能為目的，並設定特定安全管控機制（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等）。

2.7 使用者註冊

人員報到或離退職應會辦電腦系統帳號管理人員，執行電腦系統的使用 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：

 使用唯一的使用者帳號。

 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。

 保存一份包含所有帳號註冊的記錄。

 使用者調職或離職後，應移除其帳號的存取權限。

 每學期應檢查使用者帳號，以確保帳號的有效性。（參考帳號申 請單格式，文件編號 A-3）

2.8 特權管理

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。（參考系統特權帳號清單格式，文件編號 A-4）

* 1. 通行碼（Password）之使用

2.9.1 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。

2.9.2 資訊系統與服務應避免使用共用帳號及通行碼。

2.9.3 由學校發佈通行碼制定與使用規則給使用者(參考優質通行碼設 定原則與使用原則文件，文件編號：A-5)，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保密責任。

要求使用者的通行碼設定，應該包含英文字及數字，長度為 8 碼（含）以上。

2.10 通報安全事件與處理

2.10.1 資訊安全事件包括：系統被入侵、對外攻擊、針對性攻擊、散播 惡意程式、中繼站、電子郵件社交工程攻擊、垃圾郵件、命令或 控制伺服器、殭屍電腦、惡意網頁、惡意留言、網頁置換、釣魚 網頁、個資外洩等。

2.10.2 資訊安全事件等級，由輕微至嚴重區分等級如下：

符合下列任一情形者，屬 0 級事件：

(1) 未確定事件或待確認工單:來自不同計畫所使用新型技術

(A-SOC，miniSOC,…)所產生之工單，但其正確性有待確認。 (2) 其他單位所告知教育部所屬單位所發生未確定之資安事件。

(3) 教育部及區、縣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：

(1) 非核心業務資料遭洩漏。

(2) 非核心業務系統或資料遭竄改。

(3) 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：

(1) 非屬密級或敏感之核心業務資料遭洩漏。

(2) 核心業務系統或資料遭輕微竄改。

(3) 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： (1) 密級或敏感公務資料遭洩漏。

(2) 核心業務系統或資料遭嚴重竄改。

(3) 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： (1) 國家機密資料遭洩漏。

(2) 國家重要資訊基礎建設系統或資料遭竄改。

(3) 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。

2.10.3 本校任何人於校內發現異常情況或疑似資安事件，應立即向資安 業務承辦人通報，資安業務承辦人應儘速進行處理並研判事件等 級。

2.10.4 資安業務承辦人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校長，並以電話聯絡教育局(處)資訊安全 管理單位，由校長儘快召集會議研商處理的方式。(參考資安事 件通報程序，文件編號：A-6)

2.10.5 當發生無法處理之資通安全事件，應通報教育局(處)資訊安全管 理單位協助處理。

2.10.6 教育機構資安通報平台（網址： https://info.cert.tanet.edu.tw/），帳號為學校

OID： 。

2.10.7 資安通報依情報來源分為「告知通報」與「自行通報」，若收到

「告知通報」事件通知，由資安業務承辦人登入教育機構資安通

報平台，完成通報及應變作業。

2.10.8 資安事件若為校內人員自行發現，由資安業務承辦人登入教育機 構資安通報平台進行「自行通報」完成通報及應變作業。

2.10.9 資安事件須於發生後 1 小時內進行通報，0、1、2 級事件於事件 發生後 72 小時內處理完成並結案(包括通報與應變)，3、4 級事 件於事件發生後 36 小時內完成並結案。

2.10.10如有收到教育機構資安通報平台「資安預警事件」通知，由資安 業務承辦人登入教育機構資安通報平台，進行資安預警事件單處 理作業。

2.10.11相關通報應變流程請依照「教育機構資安通報應變手冊」規定辦 理。

3 實體安全

3.1 設備安置及保護

3.1.1 主機機房及電腦教室宜設置偵煙、偵熱或滅火設備（氣體式滅火 器），並禁止擺放易燃物或飲食。

3.1.2 主機機房及電腦教室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。

3.1.3 主機機房及電腦教室應實施門禁管制。

3.2 溫濕度控制

重要的資訊設備（如：主機機房等）宜有溫濕度控制措施(溫度建議控 制在 20℃~25℃，濕度建議控制在相對濕度 50%R.H.~70%R.H.)，以防止 資訊設備意外損壞。機房內應有溫濕度顯示裝置，以觀察實際之溫濕度 情況。

3.3 電源供應

重要的資訊設備（如：主機機房等）應有適當的電力保護設施，例如設 置 UPS、電源保護措施(如：穩壓器、接地等)，以免斷電或過負載而造 成損失，並設置緊急照明設備以作為停電照明之用。

3.4 纜線安全

主機機房及電腦教室內線路應考量設置保護設施(如：高架地板、線槽、 套管等)。

3.5 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，在報廢前應填寫「啟用與報廢紀錄單」， 確認已將任何敏感資料和授權軟體刪除或覆寫。（參考啟用與報廢紀錄 單格式，文件編號 A-1）

3.6 財產攜出

3.6.1 禁止資訊設備在未經授權之情況下攜離所屬區域，若需將設備攜 出，應遵守財產管理相關規定並填寫「設備進出紀錄表」。（參考 設備進出紀錄表格式，文件編號 A-7）

3.6.2 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。

4 可攜式電腦設備與媒體

4.1 公務用可攜式電腦設備(如：筆記型電腦、平板電腦、智慧型手機等)應 設定保護機制，如設定通行碼、圖形辨識、臉孔辨識或指紋辨識等。

4.2 公務用可攜式電腦設備應執行安全相關程序（如：掃毒、預設通行碼更 新、系統更新等），以防範可能隱藏的病毒或後門程式。

4.3 公務用可攜式儲存媒體(如：隨身碟、光碟、磁帶等)應依儲存資料的機 敏性實施安全控管措施，如檔案加密儲存或將該儲存媒體存放於上鎖 儲櫃或安全處所。

5 人員安全

5.1 人員安全責任 非正式人員、約聘(僱)人員者，因業務需要，而接觸公務機密、個人 權益及學校機敏資料者須填寫保密切結書。（參考切結書格式，文件編 號 A-8）

5.2 資訊安全教育與訓練

5.2.1 鼓勵資安業務承辦人參加資安管理系統相關教育訓練。

5.2.2 鼓勵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。

6 資訊業務委外管理

6.1 服務委外廠商合約之安全要求

6.1.1 在資訊業務委外合約中，應訂定委外廠商的資訊安全責任及保密 規定。

6.1.2 應要求委外廠商簽訂安全保密切結書。(參考切結書格式，文件 編號 A-9)

6.1.3 委外廠商人員到校服務時，應請其簽署委外廠商人員保密切結

書。(參考切結書格式，文件編號 A-10)

6.2 委外廠商服務異動或終止時，應中止或刪除其系統上的帳號與權限。（參 考帳號申請單格式，文件編號 A-3）

7 應對以下各項相關法令有基礎之認知，並利用各集會場合對全校師生口頭宣 導(至少一學期一次)。

7.1 智慧財產權

著作權法

7.2 個人資訊的資料保護及隱私 個人資料保護法及施行細則

7.3 刑法電腦犯罪專章

承辦人 主任 校長

## 文件編號：A-1

啟用與報廢紀錄單**(**範本**)**

□啟用 □報廢



|  |  |  |  |
| --- | --- | --- | --- |
| 執行人 |  | 執行日期 |  |
| 設備用途 |  | 設備型號 |  |
| 啟 用 檢 查 項 目 | □掃毒  □變更預設通行碼  □系統更新  □其它：  執行人： | | |
| 報 廢 檢 查 項 目 | □刪除硬碟資料(資料無法再還原)  □其它：  執行人： | | |

執行人主管覆核：

資訊工作日誌**(**範本**)**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 操 | 作 | 日 | 期： | 民國 | 年 | 月 | 日上（下）午 | 時 | 分 |
| 系 | 統 | 名 | 稱： |  |  |  |  |  |  |

|  |  |
| --- | --- |
| 操作事項 | □ 系統例行檢查  □ 系統維護  □ 系統更新操作  □ 其它： |
| 操作說明 |  |
| 系統錯誤改正措施  說明 |  |

系統管理人員(簽名)：

主管覆核(簽名)：

帳號申請單**(**範本**)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 申請人： |  |  | 申請日期： | | | |
| 所屬單位： |  |  | 分機： | | | |
| 系統名稱 | 帳號 | 申請項目 | | | | 說明 |
| □ 1. |  | □  □ | 新增  停用 | □ 刪除 □  □ 異動 □ | 重新啟用  重設通行碼 |  |
| □ 2. |  | □  □ | 新增  停用 | □ 刪除 □  □ 異動 □ | 重新啟用  重設通行碼 |  |
| □ 3. |  | □  □ | 新增  停用 | □ 刪除 □  □ 異動 □ | 重新啟用  重設通行碼 |  |
| □ 4. |  | □  □ | 新增  停用 | □ 刪除 □  □ 異動 □ | 重新啟用  重設通行碼 |  |
| □ 5. |  | □  □ | 新增  停用 | □ 刪除 □  □ 異動 □ | 重新啟用  重設通行碼 |  |
| 備註 | | | | | | |
|  | | | | | | |
| 執行紀錄 | | | | | | |
| 資訊組長（教師）： 主管覆核： | | | | | | |

## 帳號使用注意事項

1. 使用者須妥善保管帳號通行碼，不可告知他人或書寫於他人可取得之處，如 便條紙、螢幕或主機外殼等，亦應避免放置於其他易遭他人窺視之場所。

2. 使用者通行碼的長度最少應由 8 個字元組成，並且英文與數字混和。

3. 使用者通行碼應避免包含使用者相關之個人資訊，如電話號碼、生日或姓名。

4. 使用者通行碼宜定期變更，並避免重複使用或循環使用舊通行碼。

5. 使用者離職須移除其系統帳號始完成離職手續。

系統特權帳號清單**(**範本**)**

填寫日期：

|  |  |  |
| --- | --- | --- |
| 系統名稱 | 帳號 | 人員姓名 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

填寫人： 主管覆核：

## 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通行碼。

4. 使用技巧記住通行碼

- 使用字首字尾記憶法：

* + 1. My favorite student is named Sophie Chen，取字頭成為 mFSinsC
    2. 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

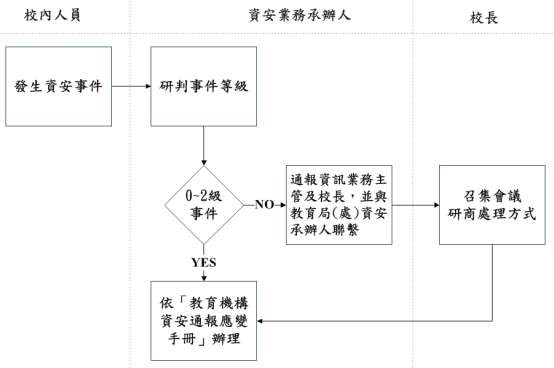
7. 避免全部使用數字，例如 52526565

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。

## 資安事件通報程序



|  |  |  |
| --- | --- | --- |
| 人員 | 姓名 | 聯絡電話 |
| 資安業務承辦人 |  |  |
| 資安業務主管 |  |  |
| 校長 |  |  |
| 教育局(處)資安承辦人 |  |  |
| 臺灣學術網路危機  處理中心(TACERT) |  |  |

填表日期： 年 月 日

設備進出紀錄表**(**範本**)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| □攜入  □攜出 | 日期  時間 | 年 月 日  時 分 | | 攜入/出人員  單 位 |  |
| 設備名稱 |  | | | 設備序號 |  |
| 設備  品牌/規格 |  | | | | |
| 攜入/出方式 | □自行攜入/出  □貨運代送(公司名稱/電話： 貨運編號： )  □其他(請說明： ) | | | | |
| 攜入/出原因 | □備份媒體異地儲存  □異地儲存之備份媒體送回  □新增設備  □設備送修(預計修復完成日期： / / )  □調 / □借 / □還  其他單位： 聯 絡 人： 聯絡電話：  （預計歸還日期： / / ）  □其他(請說明： ) | | | | |
| 覆核單位 | | | | | |
| 承辦人 | | | 權責主管 | | |
|  | | |  | | |

保密切結書**(**範本**)**

(以下簡稱為本人)擔任稻香國小之 職務。本人願於學校服務期間所接觸或處理之學校資料(凡屬與公務機密、個人 權益及學校機敏資料)，嚴守工作保密規定與國家相關法令對業務機密要求，並 負保密之責；相關資料均以於校內處理為原則，未經書面許可絕不以各種方式攜 出校外及對外揭露，若因本人造成學校損失，同意無異議接受相關法律責任，並 負責所產生各項損失賠償，離職後亦同；並尊重智慧財產權，絕不擅自下載、複 製與傳播任何侵害智慧財產權之任何程式、軟體，如有違反願自負法律責任。此 致

稻香國小

切結人： 身分證字號： 戶籍地址：

日期： 年 月 日

本保密切結書一式兩份，分別由切結人以及稻香國小保存

# 服務委外單位服務暨保密切結書**(**範本**)**

公司(以下簡稱為本公司)為配合 稻香國小 （以下簡稱為 貴校）之業務需求，本公司提供服務項目如下：

一、 二、 三、

(註：列出公司將會提供之服務項目)

本公司願於 貴校提供上述服務項目時，遵守 貴校資訊安全相關規範，所知悉 貴 校機密或任何不公開之文書、電子資料、圖畫、消息、物品或其他資訊，將恪遵 保密規定，未經 貴校書面授權，不得以任何形式利用或洩漏、告知、交付、移 轉予任何第三人，如有違誤願負法律上之責任。此致

稻香國小

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 稻香國小 學校保存

# 委外廠商人員保密切結書**(**範本**)**

(以下簡稱為本人)任職於 (委外公司名稱)，因執行 工作，於 貴校執行 服務期間，願遵守 貴校資訊安全相關規範，並對所知悉 貴校機密或 任何不公開之文書、電子資料、圖畫、消息、物品或其他資訊，將恪遵 保密規定，未經 貴校書面授權，不得以任何形式利用或洩漏、告知、 交付、移轉予任何第三人，如有違誤願負法律上之責任。此致

稻香國小

切結人： 任職公司： 公司統一編號：

## 日期： 年 月 日

本保密切結書一式兩份，分別由切結人以及 稻香國小 學校保存