

臺南市東區勝利國小

資通安全管理規範

中 華 民 國 102 年 09 月 23 日

臺南市立東區勝利國小資通安全管理辦法

民國 102 年 01 月 16 日校務會議通過

民國 102 年 09 月 23 日校務會議修改通過

一、依據

- 教育部 96 年 5 月 30 日函頒國中、小學資通安全管理制度系統實施原則。
- 個人資料保護法
中華民國 101 年 9 月 21 日行政院院臺法字第 1010056845 號令發布除第 6、54 條條文外，其餘條文定自一百零一年十月一日施行。
- 個人資料保護法施行細則
中華民國 101 年 9 月 26 日法務部法令字第 10103107360 號令修正發布名稱及全文 33 條；並自一百零一年十月一日施行。
- 教育部資訊及科技教育司 100 年度教育機構個人資料保護工作事項暨檢核表。

二、目的

本規範為確保臺南市立東區勝利國民小學（以下簡稱本校）所屬之資訊資產機密性、完整性及可用性，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅。

三、適用範圍

本校校內電腦、資訊與網路服務相關的系統、設備、程序及人員，包含合約廠商及其它經授權使用之人員。

四、組織與職權

為強化本校資通安全暨個資保護需求，健全資通安全管理制度，特設立「**臺南**
市東區勝利國小資通安全委員會」（以下簡稱本委員會），以推動本校資通

安全管理業務之運作。本委員會之成員為校長、各處室主任及行政組長，由校長兼任召集人，資訊組長（網管）為資通安全長，行政及技術相關事宜由資訊組負責。

本委員會權責如下：

1. 訂定本校資通安全政策及資通安全管控機制。
2. 督導資通安全政策之實施。
3. 資通安全事件通報、緊急應變及危機處理。
4. 規劃並督導資通安全教育訓練。
5. 督導個人資料保護工作之落實。

本委員會每年開會一次，必要時得召開臨時會議。會議須有應出席委員半數(含)以上出席始得開會，並得邀請相關人員列席。

五、 資安政策

維護本校資訊之機密性、完整性與可用性，保障使用者資料隱私。

- 保護本校網路資訊，避免未經授權的存取與修改。
- 本校業務執行須符合相關法令及法規之要求。
- 建立資訊業務永續運作計畫，確保本校業務永續運作。

六、 實施規定

1. 網路安全

1.1 網路控制措施

- 本校與外界連線，應僅限於經由教育局網路管理單位之管控，以符合一致性和單一性之安全要求。
- 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

- 委外開發或維護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（電子郵件、網站主機）、教學系統主機（例如隨選視訊主機）。
- 本校的行政系統主機（例如財務、人事、公文系統等）電腦，由教育局或市政府等單位統籌管理。

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：
 - 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。
 - 設定「Windows Update」之程式更新作業，以防範作業系統之漏洞。
- 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。（伺服主機啟用與報廢申請單格式參見文件編號 A-2）

2.3 資料備份

- 本校系統管理人員需針對學校重要系統（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；並應使用設備執行异地備份或使用光碟、隨身碟或外接式硬碟執行异地存放。

2.4 操作員日誌

- 本校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。（機房操作日誌文件參見文件編號 A-3）

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等）。

2.6 使用者註冊

- 人員報到或離退職應會辦資訊組長（教師），資訊組長（教師）應執行電腦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。(帳號申請單格式參見文件編號 A-4)

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。(特權帳號清單格式參考文件編號 A-5)

2.8 通行密碼 (Password) 之使用

- 本校各資訊系統與服務應避免使用共同帳號及密碼。
- 設定各應用系統的帳號密碼時，請遵循以下原則：
 - 混合大寫與小寫字母、數字，特殊符號。
 - 密碼越長越好，最短也應該在 8 個字以上。
 - 至少每三個月改一次密碼。
 - 使用技巧記住密碼
- 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「密碼」的注音輸入為「wj/ vu/6a83」
- **應該避免的作法**
 - a. 嚴禁不設密碼、與帳號相同或與主機名稱相同。
 - b. 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。
 - c. 不重覆電腦鍵盤上的字母，例如 6666rrrr 或 qwertyui 或 zxcvbnm。
 - d. 不使用連續或簡單的組合的字母或數字，例如 abcdefgh 或 12345678 或 24681024
 - e. 避免全部使用數字，例如 52526565。
 - f. 不使用難記以至必須寫下來的密碼。
 - g. 避免使用字典找得到的英文單字或詞語，如 TomCruz 、 superman
 - h. 不要使用電腦的登入畫面上任何出現的字。

- i. 不分享密碼內容給任何人，包括男女朋友、職務代理人、上司等。
 - j. 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密碼。
- 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，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，應該包含英文字及數字，長度為 8 碼(含)以上。
 - 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、病毒感染、垃圾郵件、資料或網頁遭竄改、以及通訊中斷等。
- 本校資訊安全事件等級，由輕微至嚴重區分等級如下：
 - 0 級：教育部及新北市政府教育局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組長（教師）通報，資訊組長（教師）應儘速進行處理並研判事件等級。
- 資訊組長（教師）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，並以電話聯絡新北市政府教育局資訊安全管理單位資安承辦人，由校長儘快召集會議研商處理的方式。
- 當本校發生無法處理之資通安全事件，應通報新北市教育局資訊安全管理單位協助處理。
- 教育機構資安通報平台（網址：<https://info.cert.tanet.edu.tw/>），帳號為學校 OID：2.16.886.111.90028.90001.100004。
- 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，由資訊組長（教師）登入教育機構資安通報平台，完成通報及應變作業。
- 資安事件若為校內人員自行發現，由資訊組長（教師）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。
- 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。
- 如有收到教育機構資安通報平台「資安預警情報」事件通知，由資訊組長（教師）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。
- 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

- 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，應設置偵煙、偵熱與滅火設備（氣體式滅火器），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，應於入出口處設置門禁的機制。

3.2 溫濕度控制

- 本校重要的資訊設備（如主機機房）應有溫濕度控制措施，以防止資訊設備意外損壞，溫度最好控制在 20°C~25°C，濕度最好控制在相對濕度 50 度~70 度。機房內應懸掛溫濕度計，以觀察實際之溫濕度情況。

3.3 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，並設置緊急照明設備以作為停電照明之用。

3.4 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設置保護設施。

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，在報廢前應先確保已將任何敏感資料和授權軟體刪除或覆寫。

3.6 設備維護

- 若有必要，宜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。

3.7 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。
- 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。
- 相關財產之攜出應依教育部或學校既有之相關規定處理。

3.8 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、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，如個人鑰匙、個人密碼以及螢幕保護，螢幕保護啟動時間必須 10 分鐘或是更少。

4. 人員安全

4.1 人員安全責任

- 利用各種場合宣導各層級人員應負之資訊安全責任，每學年至少要於校務會議上宣導一次本管理辦法，以及重要資通安全消息，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、校外教學等），廠商必須簽訂安全保密切結書。
- 本校臨時人員及志工因業務需要，而接觸公務機密、個人及事業單位權益相關之資料者須填寫校內人員保密切結書。（切結書格式參見文件編號 A-6）

4.2 資訊安全教育與訓練

- 本校資通安全長，每年至少要有十八小時的資通安全相關教育訓練，使其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。
- 其他教職員工每年至少要有六小時，參與資通安全教育訓練或宣導活動，以提昇資通安全認知。

5. 個資保護要求

5.1 本校應就法律允許下，因公務需求所蒐集、處理及保存的個人資料，公佈以下項目至學校網站上。

- 個人資料檔案名稱。
- 保有機關名稱及聯絡方式。
- 個人資料檔案保有之依據及特定目的。
- 個人資料之類別。

5.2 本校教職員工必須遵守個資法規定，不得以任何理由，在沒有法源依據或違反當事人的意願下任意蒐集或洩露他人個資。

5.3 個資法實施後，本校辦理各項活動之因應措施

- 本校在辦理任何公開活動，會有蒐集、處理甚至公佈部份個資(例：姓名)時，必須在活動辦法及報名表中，陳述「本校之機關名稱」、「蒐集用途」及「使用地區和期限」，在經「當事人同意」並報名後始得蒐集。若有公佈的需求時，必須加註「將會公佈本活動優勝人（學）員名單」字樣。**所蒐集的個資，必須於宣告期限後予以銷毀。**
- 本校承辦業務人員，必須妥善保護各項個人資料，並在活動辦法及報名表中註明**「本校將會善盡保管之責」**字樣。

6. 應對以下各項相關法令有基礎之認知

6.1 智慧財產權

- 經濟部智慧財產局
<http://www.tipo.gov.tw/>
- 著作權法
<http://law.moj.gov.tw/LawClass/LawContent.aspx?PCODE=J0070017>

6.2 個人資料保護及隱私

- 個人資料保護法

- 個人資料保護法施行細則
<http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050022>

6.3 電子簽章法

- 電子簽章法
<http://law.moj.gov.tw/LawClass/LawContent.aspx?PCODE=J0080037>
- 電子簽章法施行細則
<http://law.moj.gov.tw/LawClass/LawContent.aspx?PCODE=J0080039>
- 核可憑證機構名單
<http://gcis.nat.gov.tw/eclaw/bbs.asp>

承辦人



單位主管



校長



文件編號：A-1

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 臺南市東區勝利國小
(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

臺南市東區勝利國小

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_____公司以及臺南市東區勝利國小保存

文件編號：A-2

伺服主機啟用與報廢申請單

申請人		申請日期	
伺服主機用途		項目	<input type="checkbox"/> 啟用 <input type="checkbox"/> 報廢
啟用檢查項目	<input type="checkbox"/> 掃毒 <input type="checkbox"/> 更新系統密碼	執行人：	
報廢檢查項目	<input type="checkbox"/> 刪除硬碟資料	執行人：	

執行人主管覆核：

文件編號：A-3

機房操作日誌

填寫日期： 民國____年____月____日
系統操作起始時間： 上(下)午____時____分
系統操作結束時間： 上(下)午____時____分

操作事項	<input type="checkbox"/> 系統例行檢查 <input type="checkbox"/> 系統維護 <input type="checkbox"/> 系統更新操作
系統錯誤說明	
採取改正措施說明	

操作人員： _____ 簽名欄 _____

日誌填寫人員： _____ 簽名欄 _____

帳號申請單

申請人		申請日期		
所屬單位		分機		
系統名稱	帳號	申請項目		
□ 1.		<input type="checkbox"/> 新增	<input type="checkbox"/> 刪除	<input type="checkbox"/> 重新啟用
		<input type="checkbox"/> 停用	<input type="checkbox"/> 異動	<input type="checkbox"/> 重設密碼
□ 2.		<input type="checkbox"/> 新增	<input type="checkbox"/> 刪除	<input type="checkbox"/> 重新啟用
		<input type="checkbox"/> 停用	<input type="checkbox"/> 異動	<input type="checkbox"/> 重設密碼
□ 3.		<input type="checkbox"/> 新增	<input type="checkbox"/> 刪除	<input type="checkbox"/> 重新啟用
		<input type="checkbox"/> 停用	<input type="checkbox"/> 異動	<input type="checkbox"/> 重設密碼
□ 4.		<input type="checkbox"/> 新增	<input type="checkbox"/> 刪除	<input type="checkbox"/> 重新啟用
		<input type="checkbox"/> 停用	<input type="checkbox"/> 異動	<input type="checkbox"/> 重設密碼
□ 5.		<input type="checkbox"/> 新增	<input type="checkbox"/> 刪除	<input type="checkbox"/> 重新啟用
		<input type="checkbox"/> 停用	<input type="checkbox"/> 異動	<input type="checkbox"/> 重設密碼
申請權限				
執行紀錄				
資訊組長（教師）：				

帳號使用注意事項

- 使用者須妥善保管帳號密碼，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。
- 使用者密碼的長度最少應由 8 個字元組成，並且英文與數字混和。
- 使用者密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。
- 使用者密碼宜定期變更，並避免重複使用或循環使用舊密碼。
- 使用者離職須移除其系統帳號始完成離職手續。

文件編號：A-5

系統特權帳號清單

填寫日期：

填寫人：

主管覆核：

文件編號：A-6

校內人員保密切結書

(以下簡稱為本人)擔任臺南市東區勝利國小之職務。本人願意在學校執行業務時，存取學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；相關資料均以留在學校內部處理，未得許可絕不以各種方式攜出校外及對外透露。

本人亦不私自蒐集學校所擁有之任何資訊，若因本人造成學校損失，同意無異議接受相關法律責任，並負責所引發之各項損失賠償。此致

臺南市東區勝利國小

簽署人：

姓名：

身分證統一編號：

戶籍地址：

日期： 年 月 日

本保密切結書一式兩份，分別由簽署人以及臺南市東區勝利國小學校保存