桃園市新屋區永安國民中學

105 年度國中資通安全管理規範

中 華 民 國 105 年 12 月 08 日

桃園市新屋區永安國中資通安全管理系統實施原則

一、 文件目標

本文件依據「教育部國中、小學資通安全管理系統實施原則」，提供作為本校資通安全管理規範，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、 實施原則

1. 網路安全

1.1 網路控制措施

- 學校與外界連線，應僅限於經由縣網中心之管控，以符合一致性與單一性之安全要求。
- 學校內特殊系統（例如會計系統、學生學籍、成績原始資料系統等）之資料，當有必要透過網路進行傳輸時，建議透過虛擬私有網路（Virtual Private Network, VPN）或同等連線方式進行；若無透過網路進行傳輸需求，則建議區隔於網路之外。
- 應禁止以電話線連結主機電腦或網路設備。

1.2 網路安全管理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（參考切結書範本，文件編號 A-1）。

2. 系統安全

2.1 職責區隔

- 學校主機電腦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）。
- 學校的行政系統主機（例如財務、人事、公文系統等）電腦，建議由各個縣（市）教育網路中心或教育局等單位統籌管理。

2.2 對抗惡意軟體、隱密通道及特洛依木馬程式

- 學校內的個人電腦應：
  - 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
  - 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
- 學校內個人電腦所使用的軟體應有授權。
- 新系統啟用前，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

- 學校(或委託)系統管理人員需針對學校重要系統（例如系統檔案、應用系統、資料庫等）定期進行備份工作，或採用自動備份機制；建議週期為每週進行一次。

2.4 操作員日誌

- 學校(或委託)系統管理人員需針對敏感度高、或包含特殊資訊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。
- 日誌內容可包含以下各項：
  - 系統例行檢查、維護、更新活動的起始時間

- 系統錯誤內容和採取的改正措施。[參考日誌範本，文件編號 *A-2*]
- 紀錄日誌項目人員姓名與簽名欄

2.5 資訊存取限制

- 學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

- 學校應制定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。
  - 定期（建議每學期）檢查並取消多餘的使用者識別碼和帳號。
  - 定期（建議每學期）檢查新增之帳號，若有莫名帳號產生，應關閉帳號權限，並依通報程序請求處理（參照本文件 2.10 段落）。

2.7 特權管理

- 學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，[參考優質通

  行碼設定原則與使用原則，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 原始程式庫之存取控制

- 學校與系統廠商間的合約應加註對原始程式庫安全之要求，並防範資料庫隱碼(SQL-injection)問題，針對存取資料庫程式碼之輸入欄位進行字元合理性檢查。

2.10 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。
- 學校應建立資訊安全事件通報程序[參照安全事件通報程序，編號 *A-4*]以及安全事件通報單[參考安全事件通報單範本，文件編號 *A-5*]；通報程序應包括學校內部通報，以及學校與所屬縣市教育網路中心的通報。
- 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。

3. 實體安全

3.1 設備安置及保護

- 學校重要的資訊設備（如主機機房）應置於設有空調空間。
- 學校資訊設備主機機房、電腦教室區域，應設置滅火設備，並禁止擺放易燃物、或飲食。
- 學校資訊設備主機機房、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。
- 學校資訊設備主機機房、電腦教室區域，應至少於入出口處加裝門鎖或其他同等裝置。

3.2 電源供應

- 學校重要的資訊設備（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

- 學校資訊設備主機機房、電腦教室區域內應避免明佈線。

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

- 應與設備廠商建立維護合約。
- 廠商進入安全區域需簽訂安全保密切結書。

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。
- 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。

3.7 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（例如公文、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。
- 學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。

1. 人員安全

1.1 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，以強化工作上之資訊安全意識。

- 因業務需要將機敏資料攜出機關時（如郵寄廠商、校外教學等），應簽署資料攜出保密切結書。
- 本校編制人員及志工因業務需要，而接觸公務機密、個人及專業單位相關之資料者須填寫校內人員保密切結書

1.2 資訊安全教育與訓練

- 本校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，並熟悉資安事件通報之程序。
- 本校鼓勵資訊部門人員(系統管理人員以及所有校職員參與資訊安全教育訓練或宣導活動，以提升資訊安全認知。

2. 應符合下各項相關法令有基礎之認知

2.1 智慧財產權

- 著作權法

2.2 個人資訊的資料保護及隱私

- 個人資料保護法
- 個人資料保護法施行細則

承辦人：　　單位主管：　　校長：

桃園市新屋區永安國中資通安全管理系統實施原則

一、 文件目標

本文件依據「教育部國中、小學資通安全管理系統實施原則」，提供作為本校資通安全管理規範，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、 實施原則

4. 網路安全

4.1 網路控制措施

- 學校與外界連線，應僅限於經由縣網中心之管控，以符合一致性與單一性之安全要求。
- 學校內特殊系統（例如會計系統、學生學籍、成績原始資料系統等）之資料，當有必要透過網路進行傳輸時，建議透過虛擬私有網路（Virtual Private Network, VPN）或同等連線方式進行；若無透過網路進行傳輸需求，則建議區隔於網路之外。
- 應禁止以電話線連結主機電腦或網路設備。

4.2 網路安全管理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（參考切結書範本，文件編號 A-1）。

5. 系統安全

5.1 職責區隔

- 學校主機電腦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）。
- 學校的行政系統主機（例如財務、人事、公文系統等）電腦，建議由各個縣（市）教育網路中心或教育局等單位統籌管理。

5.2 對抗惡意軟體、隱密通道及特洛依木馬程式

- 學校內的個人電腦應：
  - 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
  - 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
- 學校內個人電腦所使用的軟體應有授權。
- 新系統啟用前，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。

5.3 資料備份

- 學校(或委託)系統管理人員需針對學校重要系統（例如系統檔案、應用系統、資料庫等）定期進行備份工作，或採用自動備份機制；建議週期為每週進行一次。

5.4 操作員日誌

- 學校(或委託)系統管理人員需針對敏感度高、或包含特殊資訊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。
- 日誌內容可包含以下各項：
  - 系統例行檢查、維護、更新活動的起始時間

- 系統錯誤內容和採取的改正措施。[參考日誌範本，文件編號 *A-2*]
- 紀錄日誌項目人員姓名與簽名欄

5.5 資訊存取限制

- 學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）。

5.6 使用者註冊

- 學校應制定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。
  - 定期（建議每學期）檢查並取消多餘的使用者識別碼和帳號。
  - 定期（建議每學期）檢查新增之帳號，若有莫名帳號產生，應關閉帳號權限，並依通報程序請求處理（參照本文件 2.10 段落）。

5.7 特權管理

- 學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。

5.8 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，[參考優質通

  行碼設定原則與使用原則，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。

5.9 原始程式庫之存取控制

- 學校與系統廠商間的合約應加註對原始程式庫安全之要求，並防範資料庫隱碼(SQL-injection)問題，針對存取資料庫程式碼之輸入欄位進行字元合理性檢查。

5.10 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。
- 學校應建立資訊安全事件通報程序[參照安全事件通報程序，編號 *A-4*]以及安全事件通報單[參考安全事件通報單範本，文件編號 *A-5*]；通報程序應包括學校內部通報，以及學校與所屬縣市教育網路中心的通報。
- 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。

6. 實體安全

6.1 設備安置及保護

- 學校重要的資訊設備（如主機機房）應置於設有空調空間。
- 學校資訊設備主機機房、電腦教室區域，應設置滅火設備，並禁止擺放易燃物、或飲食。
- 學校資訊設備主機機房、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。
- 學校資訊設備主機機房、電腦教室區域，應至少於入出口處加裝門鎖或其他同等裝置。

6.2 電源供應

- 學校重要的資訊設備（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。

6.3 纜線安全

- 學校資訊設備主機機房、電腦教室區域內應避免明佈線。

6.4 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。

6.5 設備維護

- 應與設備廠商建立維護合約。
- 廠商進入安全區域需簽訂安全保密切結書。

6.6 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。
- 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。

6.7 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（例如公文、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。
- 學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。

2. 人員安全

2.1 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，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。

2.2 資訊安全教育與訓練

- 本校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。
- 本校鼓勵資訊組長/老師/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。

3. 應對以下各項相關法令有基礎之認知

3.1 智慧財產權

- 著作權法

3.2 個人資訊的資料保護及隱私

- 個人資料保護法
- 個人資料保護法施行細則

承辦人： 單位主管： 校長：

文件編號：A-1

桃園市新屋區永安國中啟用與報廢紀錄單

□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：

文件編號：A-2

桃園市新屋區永安國中資訊工作日誌

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)：_____

文件編號：A-3

桃園市新屋區永安國中帳號申請單

申請人：		申請日期：	
所屬單位：		分機：	
系統名稱	帳號	申請項目	說明
☐ 1.		☐ 新增 ☐ 刪除 ☐ 重新啟用 ☐ 停用 ☐ 異動 ☐ 重設通行碼	
☐ 2.		☐ 新增 ☐ 刪除 ☐ 重新啟用 ☐ 停用 ☐ 異動 ☐ 重設通行碼	
☐ 3.		☐ 新增 ☐ 刪除 ☐ 重新啟用 ☐ 停用 ☐ 異動 ☐ 重設通行碼	
☐ 4.		☐ 新增 ☐ 刪除 ☐ 重新啟用 ☐ 停用 ☐ 異動 ☐ 重設通行碼	
☐ 5.		☐ 新增 ☐ 刪除 ☐ 重新啟用 ☐ 停用 ☐ 異動 ☐ 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。

文件編號：A-4

桃園市新屋區永安國中系統特權帳號清單

填寫日期：

系統名稱	帳號	人員姓名

填寫人：　　主管覆核：

文件編號：A-5

桃園市新屋區永安國中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：
     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」

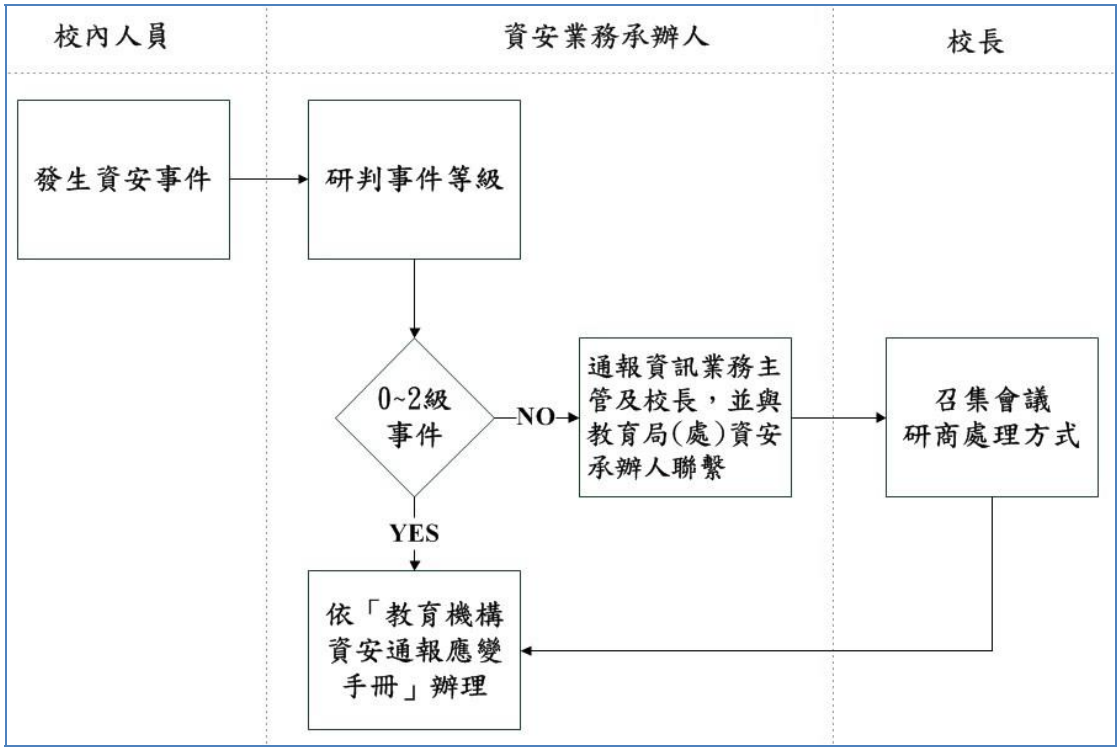
二、 應該避免的作法

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 xcvbnm。
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。

文件編號：A-6

桃園市新屋區永安國中資安事件

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)		

文件編號：A-7

桃園市新屋區永安國中設備進出紀錄表

填表日期：　年　月　日

□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		

文件編號：A-8

桃園市新屋區永安國中保密切結書

_____(以下簡稱為本人)擔任桃園市新屋區永安國中職務。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

桃園市新屋區永安國中

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，分別由切結人以及學校保存

文件編號：A-9

桃園市新屋區永安國中服務委外單位服務暨保密切結書

_____公司(以下簡稱為本公司)為配合學校（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

桃園市新屋區永安國中

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_____公司以及學校保存

文件編號：A-10

桃園市新屋區永安國中委外廠商人員保密切結書

_____ (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

桃園市新屋區永安國中

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，分別由切結人以及學校保存