高雄市美濃區廣興國小資訊安全管理辦法

壹、依據

高雄市美濃區廣興國民小學（以下簡稱本校）為推動資訊安全教育，強化資訊安全管理，確保資料、系統、設備及網路安全，依據『行政院及所屬各機關資訊安全管理要點』，訂定本辦法。

貳、目標

一、 維護校園網路環境安全與網路服務正常運作。

二、建立重要資料安全存取程序避免資料外洩。

三、推廣並實施資訊安全教育，建立正確使用資訊態度。

參、實施範圍

一、 人員：本校教職員工、學生及使用本校系統資源之委外廠商人員。

二、 應用系統：包含校務系統、公文系統、校園網路服務等。

三、 硬體設備：所有校內電腦主機、伺服器及網路資訊設備。

四、 教育宣導：利用教師晨會時間宣導資訊安全，並舉行相關研習，及利用資訊課程實施資訊素養相關教育。

肆、權責與分工

本校資訊安全工作之權責分工如下：

一、 資訊安全政策、計畫及規範之建置及評估等事項，由資訊組負責辦理。

二、 資訊設備之保全由各保管使用者負責。

三、 重要資料之保管與維護，由各業務承辦人員負責辦理。

四、 資訊安全教育由本校全體教師共同辦理。

伍、安全管理

一、 電腦病毒及惡意軟體之防範

1.購置安裝防毒軟體，防制及偵測電腦病毒及惡意軟體。

2.電腦病毒防範應考量的重要原則

3.防毒軟體及病毒碼應定期更新版本。

4.應定期或即時掃瞄電腦系統及資料儲存媒體。

5.對來路不明及內容不確定的磁碟，應在使用前詳加檢查是否感染電腦病毒。

6.應定期將必要的資料備份。

二、電腦軟體授權與管理

1.軟體採購由業務單位負責與管理。

2.禁止教職員工及學生安裝使用未取得授權的軟體。

三、 日常作業之安全管理

1.應定期執行必要的資料及軟體備份，以便發生災害或是儲存媒體失效時，可迅速回復正常作業。

2.電腦軟硬體及網路系統出現問題時，應通知相關人員或資訊組處理。

3.電腦軟硬體及網路系統更新、維修、問題處理應定期記錄，以供日後查考。

四、 資料安全之管理

1.電腦媒體之使用管理：

(1)包括可攜帶移動的磁碟、光碟、筆記型電腦等，應依保存規格要求，存放在安全的環境。媒體儲存的資料，不再繼續使用時，應將儲存的內容消除。

(2)內含機密性或敏感性資料的媒體報廢時，應以安全的方式處理，例如：燒毀、以碎紙機處理，或將資料從媒體中完全清除。

2.處理、收受機密性、敏感性的資料，應防範洩漏或不法及不當的使用，視各業務單位之需求，可於獨立的或是專屬的電腦中執行，或在傳輸、儲存過程中以加密方法保護。

3.電子檔案之保管

(1)電子資料檔案應妥善保管定期備份，以防止遺失、損毀、或不當使用。

(2)超過保存時限的檔案，應依相關規定刪除或銷毀。

五、 網路安全管理

1.本校教職員工及學生，依其身分及所執行之工作及學習行為，為合法授權之校園網路使用者，並遵守下列規定：

(1)不得將自己的登入身份識別帳號與密碼交付他人使用。

(2)不得使用他人的登入身份識別帳號與密碼。

(3)禁止利用校園網路從事不法、不當得利之情事。

(4)網路使用者不得以任何手段蓄意干擾或妨害校園網路的正常運作。

2.為避免重要資料被竊或外流，依規定不得安裝 P2P 軟體於校內任何主機，確保資料安全及網路正常運作。

3.機密性及敏感性的資料或文件，不得存放在對外開放的資訊系統中。

4.資訊安全事件緊急應變之處理

若發現網路被入侵或疑似被入侵時(如：網頁遭竄改、分散式攻擊、資料非法存取、密碼被破解等)，應立即依下列程序處理，並採取必要的行動。

(1)立即切斷入侵者的網路連接，如無法切斷則必須關閉防火牆。

(2)應全面檢討網路安全措施及修正防火牆的設定，以防範類似的入侵與攻擊。

(3)應正式記錄入侵的情形及評估影響的層面。

(4)立即向權責主管人員報告入侵情形。

(5)事件發生 72 小時內依規定完成通報，以獲取必要的外部協助，並儘快完成系統修復。

六、 網路安全稽核

1.網路安全稽核事項

(1)操作紀錄及作業紀錄應予以保存。

(2)對於通過防火牆之各項連線資訊，均應予記錄。

(3)各伺服主機應記載各項連結服務的作業紀錄(system log)。

七、 使用者之註冊及使用理管理

1.對於多人使用的資訊系統(校務系統、公文系統、校、班級網頁)，必須依循安全的註冊程序。

2.帳號及權限管理，必須考量的事項如下：

(1)確認使用者是否已經取得使用資訊系統之正式授權。

(2)確認使用者被授權的程度是否與業務目的相稱，是否符合資訊安全政策及規定，再依執行業務之需求，賦予使用者系統存取特別權限。

(3)使用者調整職務及離（休）職時，必須儘速註銷其系統存取權限。

(4)確認系統存取特別權限之事項以及人員名單，定期檢查及取消閒置不用的帳號。

3.密碼之管理

(1)使用者個人必須負責保護密碼，以維持其機密性。

(2)避免將通行密碼記錄在書面上，或張貼在個人電腦或終端機螢幕或其他容易洩漏秘密之場所。

(3)當有跡象足以顯示系統及使用者密碼可能遭破解時，應立即更改密碼。

(4)密碼的長度最少應由六位長度組成(不得為空白)。

(5)更換維護廠商時，防火牆及主機之相關帳號及密碼須刪除或修改。

八、 設備安全管理

1.設備應安置在適當地點，以減少環境不安全引發之危險及未經授權存取系統的機會。

2.設備安置應遵循的原則如下：

(1)設備應儘量安置在不需經常進出之地點。處理機密性資料工作站，應放置在可注意及可就近照顧之地點。

(2)需特別保護之設備，應考量與一般設備區隔。

(3)應檢查及評估火災、煙、水、灰塵、震動、化學效應、電力供應、電磁幅射等加諸於設備之危害。

(4)電腦作業區應禁止抽煙及飲用食物。

(5)應考量其他可能導致之危險因素。

3.辦公桌面之安全管理

(1)公文及磁碟長時間不使用及下班後，應妥為存放；機密性、敏感性資訊，應妥為收存。

(2)棄置之手寫或影印公文廢紙及已過保存期限之公文，應視需要予以銷毀。

(3)個人電腦及終端機不使用時，應予關機、登出、設定螢幕密碼或是以其他控制措施保護。

九、無線網路存取

1.校內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。

2.校內提供無線網路存取服務，並採取適當安全管控措施：

(1).專供行政使用之無線網路熱點已設定加密金鑰防護，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。

(2) 於教學區域、會議室等場所佈建之無線網路熱點已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。

(3) 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（I TAIWAN），網段與校園網路隔離。

十、**可攜式電腦設備與媒體**

（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。

（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。

（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。

十一、資訊業務委外管理

服務委外廠商合約之安全要求

（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。

（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）

（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）

（4）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）

陸、資訊安全事件通報處理機制

一、 資訊安全事件之通報

1. 因資訊安全事件（包括系統有安全漏洞、遭受非法入侵及破壞、遭遇阻斷服務攻擊及功能不正常事件等），致電腦系統無法運作或影響執行效率時，相關人員應視其狀況嚴重程度及影響層面，循序向各權責主管報告。
2. 資訊組發現有資訊安全事件時，應依資訊安全事件通報管道（如：教育機構資安通報平台），迅速通報權責主管單位及人員處理。

二、 通報後應採行之措施

1. 應立即停止使用受影響之電腦系統或設備，並保留現況。
2. 負責人員接獲通報後應紀錄相關的訊息。
3. 系統管理人員處理後，應向直屬業務主管回報處理結果，並作成紀錄。

三、 緊急應變計畫

1. 人員請假或有緊急事故時，可將重要事項交託職務代理人代為處理，若需人員親自處理時，可透過電話聯繫及網路連線作必要之處置。
2. 系統方面緊急應變措施：定期執行資料及軟體之備份及備援作業，以便發生災害或是儲存媒體失效時，可迅速回復正常作業。

柒、本計畫經校長核可後經校務會議通過後實施，修正時亦同。

承辦人：古錦明　　教務主任：教師兼任教務處主任溫文玲　　校長：高雄市美濃區民族國民小學校長謝惠君

總務主任：教師兼任總務處主任林勤博

文件編號：A-3

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。

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-8

保密切結書

＿＿＿＿＿＿＿＿＿＿(以下簡稱為本人)擔任廣興國小之＿＿＿＿＿＿＿＿＿＿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

廣興國小

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＿＿＿＿＿＿學校保存

文件編號：A-9

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

廣興國小

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＿＿＿＿＿＿學校保存

文件編號：A-10

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

廣興國小

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_____學校保存