國立苑裡高級中學資通安全維護計畫附件

目　次

1. 資通安全推動小組成員及分工表

國立苑裡高級中學資通安全推動小組成員及分工表

編號：○○

製表日期：108年○○月○○日

國立苑裡高級中學資通安全推動小組成員及分工表

單位職級	職掌事項	分機	備註（代理人）
校長	督導資通安全工作	101	秘書
圖書館主任	統籌資通安全相關業務	800	資訊媒體組組長
秘書	協助資安工作	101	
教務主任	協助資安工作	200	教學組長
學務主任	協助資安工作	300	訓育組長
總務主任	協助資安工作	500	庶務組長
輔導主任	協助資安工作	400	資料輔導組組長
人事主任	協助資安工作	700	
會計主任	協助資安工作	600	
教學組長	協助資安工作	201	
訓育組長	協助資安工作	304	
庶務組長	協助資安工作	501	
資料輔導組組長	協助資安工作	401	

資訊媒體組組長	資通安全專責人員	801	圖書館職員
圖書館職員	資通安全事件處理	802	

資通安全長：校長

2. 資通安全保密同意書

國立苑裡高級中學資通安全保密同意書

編號：○○

立同意書人 ○○○ 於民國 ○○ 年 ○○ 月 ○○ 日起於 ○○ 任職，因業務涉及單位重要之資訊及資通系統，故同意下列保密事項：

一、於業務上所知悉之機敏資料及運用之資通系統等，應善盡保管及保密之責。

二、相關業務之資訊、文件，不得私自洩漏與業務無關之人員。

三、遵守其他本單位資通安全相關之法令及規定。

四、如有危害本單位資通安全之行為，願負相關之責任。

立同意書人：○○○ (簽章)

身份證字號：○○○

服務機關：○○

機關首長：○○○

中　華　民　國　　年　　月　　日

3. 資通安全需求申請單

國立苑裡高級中學資通安全需求申請單

編號：○○

申請單位	○○部門	申請日期	108年○○月○○日
申請項目	■軟體 □硬體 □其他	項目名稱	○○防毒軟體
申請數量	1	需用日期	108年○○月○○日
申請類別	■新購 □升級	使用設備	■主機 □使用者電腦 □其他
安裝單位	資訊室	安裝位置	機房
用途說明	防毒軟體更新		
申請人	○○○	單位主管	○○○
資通安全推動小組	■可採購 □不可採購	說明：	
資通安全推動小組承辦人員	○○○	資通安全長[1]	○○○

註：陳核層級請機關依需求調整

[1]特定非公務機關部分，可能是資通安全管理代表等相關資通安全負責人。

4. 管制區域人員進出登記表

國立苑裡高級中學管制區域人員進出登記表

編號：○○

製表日期：108年○○月○○日

編號	姓名	單位	陪同人員	日期	進入時間	離開時間	事由	權限	進出設備	攜帶物品
1	王○○	○○室	陳○○	106.3.1	8：00	9：00	借用電腦設備	普	手提電腦	手機

承辦人員：吳政璟　　單位主管：張明智

註：陳核層級請機關依需求調整

5. 委外廠商執行人員保密切結書、保密同意書

國立苑裡高級中學委外廠商執行人員保密切結書

立切結書人----------（簽署人姓名）等，受----------（廠商名稱）委派至----------（機關名稱，以下稱機關）處理業務，謹聲明恪遵機關下列工作規定，對工作中所持有、知悉之資訊系統作業機密或敏感性業務檔案資料，均保證善盡保密義務與責任，非經機關權責人員之書面核准，不得擷取、持有、傳遞或以任何方式提供給無業務關係之第三人，如有違反願賠償一切因此所生之損害，並擔負相關民、刑事責任，絕無異議。

一、 未經申請核准，不得私自將機關之資訊設備、媒體檔案及公務文書攜出。

二、 未經機關業務相關人員之確認並代為申請核准，不得任意將攜入之資訊設備連接機關網路。若經申請獲准連接機關網路，嚴禁使用數據機或無線傳輸等網路設備連接外部網路。

三、 經核准攜入之資訊設備欲連接機關網路或其他資訊設備時，須經電腦主機房掃毒專責人員進行病毒、漏洞或後門程式檢測，通過後發給合格標籤，並將其粘貼在設備外觀醒目處以備稽查。

四、 廠商駐點服務及專責維護人員原則應使用機關配發之個人電腦與週邊設備，並僅開放使用機關內部網路。若因業務需要使用機關電子郵件、目錄服務，應經機關業務相關人員之確認並代為申請核准，另欲連接網際網路亦應經機關業務相關人員之確認並代為申請核准。

五、 機關得定期或不定期派員檢查或稽核立切結書人是否符合上列工作規定。

六、 本保密切結書不因立切結書人離職而失效。

七、 立切結書人因違反本保密切結書應盡之保密義務與責任致生之一切損害，立切結書人所屬公司或廠商應負連帶賠償責任。

立切結書人：

姓名及簽章 身分證字號 聯絡電話及戶籍地址

立切結書人所屬廠商：

廠商名稱及蓋章　廠商負責人姓名及簽章　廠商聯絡電話及地址

填表說明：

一、 廠商駐點服務人員、專責維護人員，或逗留時間超過三天以上之突發性維護增援、臨時性系統測試或教育訓練人員（以授課時需連結機關網路者為限）及經常到機關洽公之業務人員皆須簽署本切結書。

二、 廠商駐點服務人員、專責維護人員及經常到機關洽公之業務人員每年簽署本切結書乙次。

中　華　民　國　　年　　月　　日

國立苑裡高級中學委外廠商執行人員保密同意書

茲緣於簽署人 ----------（簽署人姓名，以下稱簽署人）參與----------（廠商名稱，以下稱廠商）得標----------（機關名稱）（以下稱機關）資通業務委外案----------（案名）（以下稱「本案」），於本案執行期間有知悉或可得知悉或持有政府公務秘密及業務秘密，為保持其秘密性，簽署人同意恪遵本同意書下列各項規定：

第一條　簽署人承諾於本契約有效期間內及本契約期滿或終止後，對於所得知或持有一切機關未標示得對外公開之公務秘密，以及機關依契約或法令對第三人負有保密義務之業務秘密，均應以善良管理人之注意妥為保管及確保其秘密性，並限於本契約目的範圍內，於機關指定之處所內使用之。非經機關事前書面同意，不得為本人或任何第三人之需要而複製、保有、利用該等秘密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等秘密，或對外發表或出版，亦不得攜至機關或機關所指定處所以外之處所。

第二條　簽署人知悉或取得機關公務秘密與業務秘密應限於其執行本契約所必需且僅限於本契約有效期間內。簽署人同意公務秘密與業務秘密，應僅提供、告知有需要知悉該秘密之履約廠商團隊成員人員。

第三條　簽署人在下述情況下解除其所應負之保密義務：

原負保密義務之資訊，由機關提供以前，已合法持有或已知且無保密必要者。

原負保密義務之資訊，依法令業已解密、依契約機關業已不負保密責任、或已為公眾所知之資訊。

原負保密義務之資訊，係自第三人處得知或取得，該第三人就該等資訊並無保密義務。

第四條　簽署人若違反本同意書之規定，機關得請求簽署人及其任職之廠商賠償機關因此所受之損害及追究簽署人洩密之刑責，如因而致第三人受有損害者，簽署人及其任職之廠商亦應負賠償責任。

第五條　簽署人因本同意書所負之保密義務，不因離職或其他原因不參與本案而失其效力。

第六條　本同意書一式叁份，機關、簽署人及----------（廠商）各執存一份。

簽署人姓名及簽章：

身分證字號：

聯絡電話：

戶籍地址：

所屬廠商名稱及蓋章：

所屬廠商負責人姓名及簽章：

所屬廠商地址：

中　華　民　國　　年　　月　　日

6. 委外廠商查核項目表

國立苑裡高級中學委外廠商查核項目表

編號：○○

填表日期：○○○年○○月○○日

查核人員：○○○

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
1.資通安全政策之推動及目標訂定	1.1 是否定義符合組織需要之資通安全政策及目標？	■	□	□	已訂定資通安全政策及目標。
	1.2 組織是否訂定資通安全政策及目標？	■	□	□	政策及目標符合機關之需求。
	1.3 組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？	■	□	□	依規定按時進行教育訓練之宣達。
	1.4 組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？	■	□	□	定期進行政策及目標之檢視、調整。
	1.5 是否隨時公告資通安全相關訊息？	■	□	□	將資安訊息公告於布告欄。
2.設置資通安全推動組織	2.1 是否指定適當權責之高階主管負責資通安全管理之協調、推動及督導等事項？	■	□	□	指派副首長擔任資安長。
	2.2 是否指定專人或專責單位，負責辦理資通安全政策、計畫、措施之研議，資料、資通系統之使用管理及保護，資安稽核等資安工作事項？	■	□	□	有設置內部資通安全推動小組，並制訂相關之權責分工。
	2.3 是否訂定組織之資通安全責任分工？	■	□	□	機關內部訂有資安責任分工組織。
3.配置適當之資通安全專業人員及適當之資源	3.1 是否訂定人員之安全評估措施？	■	□	□	有訂定人員錄用之安全評估措施
	3.2 是否符合組織之需求配置專業資安人力？	■	□	□	機關依規定配置資安人員2人。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	3.3 是否具備相關專業資安證照或認證？	■	□	□	專業人員具備 ISO27001之證照
	3.4 是否配置適當之資源？	□	■	□	機關並未投入足夠資安資源。
4.資訊及資通系統之盤點及風險評估	4.1 是否建立資訊及資通系統資產目錄，並隨時維護更新？	■	□	□	依規定建置資產目錄，並定時盤點。
	4.2 各項資產是否有明確之管理者及使用者？	■	□	□	資產依規定指定管理者及使用者。
	4.3 是否定有資訊、資通系統分級與處理之相關規範？	■	□	□	資訊訂有分級處理之作業規範。
	4.4 是否進行資訊、資通系統之風險評估，並採取相應之控制措施？	■	□	□	已進行風險評估及擬定相應之控制措施。
5.資通安全管理措施之實施情況	5.1 人員進入重要實體區域是否訂有安全控制措施？	■	□	□	機房訂有門禁管制措施。
	5.2 重要實體區域的進出權利是否定期審查並更新？	□	■	□	離職人員之權限未刪除。
	5.3 電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？	□	■	□	對於進出人員並未監督其活動。
	5.4 電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及溼度狀況？	■	□	□	按時檢測機房物理面之情況。
	5.5 各項安全設備是否定期檢查？同仁有否施予適當的安全設備使用訓練？	■	□	□	依規定定期檢查並按時提供同仁安全設備之使用運練。
	5.6 第三方支援服務人員進入重要實體區域是否經過授權並陪同或監視？	□	■	□	並未陪同或監視第三方支援人員。
	5.7 重要資訊處理設施是否有特別保護機制？	□	■	□	對於核心系統主機並未設置特別保護機制。
	5.8 重要資通設備之設置地點是否檢查及評估火、煙、水、震動、化學效應、電力供應、電磁幅射或民間暴動等可能對設備之危害？	■	□	□	定期檢查物理面之風險。
	5.9 電源之供應及備援電源是否作安全上考量？	■	□	□	有設置備用電源。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	5.10 通訊線路及電纜線是否作安全保護措施？	□	■	□	電纜線老舊，並未設有安全保護措施。
	5.11 設備是否定期維護，以確保其可用性及完整性？	■	□	□	設備按期維護。
	5.12 設備送場外維修，對於儲存資訊是否訂有安全保護措施？	■	□	□	訂有相關之保護措施。
	5.13 可攜式的電腦設備是否訂有嚴謹的保護措施(如設通行碼、檔案加密、專人看管)？	■	□	□	攜帶式設備訂有保護措施。
	5.14 設備報廢前是否先將機密性、敏感性資料及版權軟體移除或覆寫？	■	□	□	設備報廢前均有進行資料清除程序。
	5.15 公文及儲存媒體在不使用或不在班時是否妥為存放？機密性、敏感性資訊是否妥為收存？	□	■	□	人員下班後並未將機敏性公文妥善存放。
	5.16 系統開發測試及正式作業是否區隔在不同之作業環境？	■	□	□	系統開發測試與正式作業區隔。
	5.17 是否全面使用防毒軟體並即時更新病毒碼？	■	□	□	按時更新病毒碼。
	5.18 是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？	■	□	□	定期進行相關系統之病毒掃瞄。
	5.19 是否定期執行各項系統漏洞修補程式？	■	□	□	定期進行漏洞修補。
	5.20 是否要求電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)？	■	□	□	系統設有檢查之機制。
	5.21 重要的資料及軟體是否定期作備份處理？	■	□	□	有定期做備份處理。
	5.22 備份資料是否定期回復測試，以確保備份資料之有效性？	■	□	□	備份資料均有測試。
	5.23 對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施？	■	□	□	均有設加密之保護措施。
	5.24 是否訂定可攜式媒體(磁帶、磁片、光碟片、隨身碟及報表等)管理程序？	■	□	□	訂有可攜式媒體之管理程序。
	5.25 是否訂定使用者存取權限註冊及註銷之作業程序？	■	□	□	訂有使用者存取權限註冊及註銷之作業程序。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	5.26 使用者存取權限是否定期檢查(建議每六個月一次)或在權限變更後立即複檢？	□	■	□	未定期檢視使用者存取權限。
	5.27 通行碼長度是否超過6個字元(建議以8位或以上為宜)？	■	□	□	通行碼符合規定。
	5.28 通行碼是否規定需有大小寫字母、數字及符號組成？	■	□	□	通行碼符合規定。
	5.29 是否依網路型態(Internet、Intranet、Extranet)訂定適當的存取權限管理方式？	■	□	□	依規定訂定適當之存取權限。
	5.30 對於重要特定網路服務，是否作必要之控制措施，如身份鑑別、資料加密或網路連線控制？	■	□	□	對於特定網路有訂定相關之控制措施。
	5.31 是否訂定行動式電腦設備之管理政策(如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求)？	■	□	□	有針對行動式電腦訂定管理政策。
	5.32 重要系統是否使用憑證作為身份認證？	■	□	□	針對重要系統設有身份認證。
	5.33 系統變更後其相關控管措施與程序是否檢查仍然有效？	■	□	□	系統更新後相關措施仍有效。
	5.34 是否可及時取得系統弱點的資訊並作風險評估及採取必要措施？	■	□	□	可即時取得系統弱點並採取應變措施。
6.訂定資通安全事件通報及應變之程序及機制	5.1 是否建立資通安全事件發生之通報應變程序？	■	□	□	有訂定通報應變程序。
	5.2 機關同仁及外部使用者是否知悉資通安全事件通報應變程序並依規定辦理？	■	□	□	同仁及委外廠商均知悉通報應變程序，並定期宣導。
	5.3 是否留有資通安全事件處理之記錄文件，記錄中並有改善措施？	■	□	□	有留存相關紀錄。
7.定期辦理資通安全認知宣導及教育訓練	7.1 是否定期辦理資通安全認知宣導？	■	□	□	有定期辦理宣導。
	7.2 是否對同仁進行資安評量？	■	□	□	按期進行資安評量。
	7.3 同仁是否依層級定期舉辦資通安全教育訓練？	■	□	□	有定期辦理教育訓練。
	7.4 同仁是否瞭解單位之資通安全政策、目標及應負之責任？	■	□	□	同仁均瞭解單位之資通安全政策及目標。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
8.資通安全維護計畫實施情形之精進改善機制	8.1 是否設有稽核機制？	■	□	□	訂有稽核機制。
	8.2 是否定有年度稽核計畫？	■	□	□	有訂定年度稽核計畫。
	8.3 是否定期執行稽核？	■	□	□	有按期執行稽核。
	8.4 是否改正稽核之缺失？	■	□	□	訂有稽核後之缺失改正措施。
9.資通安全維護計畫及實施情形之績效管考機制	10.1 是否訂定安全維護計畫持續改善機制？	■	□	□	有訂定持續改善措施。
	10.2 是否追蹤過去缺失之改善情形？	■	□	□	有追蹤缺失改善之情形。
	10.3 是否定期召開持續改善之管理審查會議？	■	□	□	定期召開管理審查會議。

製表：　　單位主管：　　資通安全長：

7. 年度資通安全教育訓練計畫

國立苑裡高級中學○○○年度資通安全教育訓練計畫

壹、依據

國立苑裡高級中學之資通安全維護計畫辦理。

貳、目的

為精進所屬人員之資通安全意識及職能，並敦促該等人員得以瞭解並執行（本機關）之資通安全維護計畫，以強化（本機關）之資通安全管理能量，爰要求該等人員應接受資通安全之教育訓練，爰擬定本教育訓練計畫。

參、實施範圍（各機關自行定義）

本機關所屬人員：

人員類別	人數
資通安全專責人員	○○
一般人員	○○
主管人員	○○
共計	○○

肆、訓練項目（各機關自行定義）

人員類別	訓練課程[2]	時數
資通安全專責人員	電子郵件安全 ○○	○○
資訊人員	資訊系統風險管理 ○○	

[2]可參考行政院國家資通安全會報技術服務中心之資安職能課程項目，網址：https://www.nccst.nat.gov.tw/Capacity?lang=zh

一般人員	資訊安全通識 ○○	○○
主管人員	○○	○○

伍、訓練期程

由各機關自行排定教育訓練期程。

陸、訓練方式

由各機關自行決定教育訓練方式(實體課程、線上課程...)。

8. 資通安全認知宣導及教育訓練簽到表

國立苑裡高級中學資通安全認知宣導及教育訓練簽到表

編號：○○○

課程名稱：資安宣導課程-案例分享、資安防護重點及社交工程等

時　　間：108年○○月○○日 8：00－9：00

地　點：　會議室

單 位	職 稱	姓 名	簽 名
人事室		○○○	
圖書館			

9. 資通安全維護計畫實施情形

國立苑裡高級中學資通安全維護計畫實施情形

編號：○○

本機關(單位)之業務因涉及全校學生個人資料檔案之持有及處理，經主管機關核定後本單位之資通安全責任等級為D級，依資通安全管理法第12條之規定，向 鈞署提出本（107）年度資通安全維護計畫實施情形、執行成果及相關說明如下表所示：

實施項目	實施內容	實施情形說明 （下列內容為範例，請機關依自身情形填寫對應的說明，並提供證明，如計畫、程序、記錄或相關公文等）
1. 核心業務及其重要性	1.1 核心業務及重要性盤點	本機關核心業務及重要性詳參資通安全維護計畫（詳附件，下同）。
2. 資通安全政策及目標之訂定	2.1 資通安全政策訂定及核定	本機關已訂定資通安全政策，詳參資通安全維護計畫，並經資安長核定(詳公文附件)。
	2.2 資通安全目標之訂定	本機關已訂定資通安全目標，詳參資通安全維護計畫。
	2.3 資通安全政策及目標宣導	本機關為推動資通安全政策，已定期向同仁及利害關係人進行宣達。
	2.4 資通安全政策及目標定期檢視	本機關已定期召開資通安全管理審查會議中檢討資通安全政策及目標之適切性 (詳會議記錄) 。
3. 設置資通安全推動組織	3.1 設定資通安全長	本機關已指定○○長為資通安全長，其職掌詳參資通安全維護計畫。
	3.2 設置資通安全推動小組	本機關已設置資通安全推動小組，其組織、分工及職常詳參資通安全維護計畫。
4. 專責人力及經費之配置	4.1 專職(責)人員配置	本機關依規定配置資通安全專職人員1人，並具備資通安全專業證照及資通安全職能評量證書各四張。另因其業務內容將涉及機密性資料，故已進行相關安全評估。

	4.2 經費之配置	本機關今年視需求已合理分資安經費，資安經費佔資訊經費之○○%。
5. 資訊及資通系統之盤點及核心資通系統、相關資產之標示	5.1 資訊及資通系統之盤點	本機關已於今年o月盤點本機關之資訊、資通系統，建立資產目錄。
	5.2 機關資通安全責任等級分級	本機關依資通安全責任等級分級辦法，為資通安全責任等級A級機關。
6. 資通安全風險評估	6.1 資通安全風險評估	本機關已於今年o月完成本機關之資訊、資通系統及相關資產之風險分析評估及處理。
	6.2 資通安全風險之因應	本機關已依資通安全風險評估之結果擬定對應之資通安全防護及控制措施。
7. 資通安全防護及控制措施	7.1 存取控制與加密機制管理	本機關已依依安全維護計畫辦理。
	7.1 作業及通訊安全管理	本機關已依依安全維護計畫辦理。
	7.2 系統獲取、開發及維護	本機關已依依安全維護計畫辦理。
	7.3 執行資通安全健診	本機關已依依安全維護計畫辦理。
8. 資通安全事件通報、應變及演練相關機制	8.1 訂定資通安全事件通報、應變及演練相關機制	本機關已依規定訂定資通安全事件通報應變程序。(詳附件)
	8.2 資通安全事件通報、應變及演練	本機關已依規定進行資通安全事件通報。 本機關已依規定於今年○、○月辦理社交工程演練，並於○月辦理通報應變演練。
9. 資通安全情資之評估及因應機制	9.1 資通安全情資之分類評估	本機關接受情資後，已進行分類評估。
	9.2 資通安全情資之因應措施	本機關已接受情資之分類，採取對應之因應措施。
10. 資通系統或服務委外辦理之管理	10.1 選任受託者應注意事項	本機關資通系統或服務委外辦理時，已將選任受託者應注意事項加入招標文件中。
	10.2 監督受託者資通安全維護情形應注意事項	本機關已依規定監督受託者資通安全維護情形，客製他資通系統開發者，已要求其出具安全性檢測證明....(請機關依實際情形列出)。
11. 資通安全教育訓練	11.1 資通安全教育訓練要求	本機關人員已規定進行資通安全教育訓練。
	11.2 辦理資通安全教育訓練	本機關已於今年o月辦理資通安全教育訓練。
12. 公務機關所屬人員辦理業務涉及	12.1 訂定考核機制並進行考核	本機關已建立考核機制，並已依規定進行平時及年終考核。

資通安全事項之考核機制		
13. 資通安全維護計畫及實施情形之持續精進及績效管理機制	13.1 資通安全維護計畫之實施	本機關已依規定訂定各階文件、流程、程序或控制措施，據以實施並保存相關之執行成果記錄。
	13.2 資通安全維護計畫實施情形之稽核機制	本機關已依規定辦理內部稽核。
	13.3 資通安全維護計畫之持續精進及績效管理	本機關已依規定辦理內部召開管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。
其他說明		

製表：　　單位主管：　　資通安全長：

10. 資通安全稽核計畫

國立苑裡高級中學○○年度資通安全稽核計畫

壹、依據

一、國立苑裡高級中學之資通安全維護計畫辦理。

二、資通安全管理法第十三條規定辦理。

貳、目的

為瞭解本機關資通安全維護計畫執行之有效性，爰擬定本稽核計畫，執行稽核作業。

參、稽核期程

每年10月進行線上自評：將資安文件佐證資料上傳至指定系統。

每年12月辦理到處室資安訪視。

肆、稽核團隊成員

邀請具備資通安全政策或該次稽核所需之技術、管理、法律或實務專業知識之公務機關代表或專家學者，稽核團隊人數原則為3至7人。

伍、稽核範圍

全校

陸、稽核項目及內容

一、資訊安全管理規範

二、網路安全

三、系統安全

四、實體安全

五、人員安全

六、相關法規與施行單位政策之符合性

柒、改善作業

對於稽核結果表現優良者給予行政獎勵，並針對缺失或待改善項目者，將前次稽核結果納入本次稽核範圍中追蹤辦理情形及進度。

11. 改善績效追蹤報告

國立苑裡高級中學改善績效追蹤報告

編號：○○

製表日期：○○○○

稽核發現			
稽核日期	108 年 10 月 20 日 08 時	受稽核單位	○○○
稽核區域	■ 電腦機房　委外業務之監督措施　自動備份系統之安全措施		
缺失或待改善項目與內容	待改善項目：電腦機房所設置之預備電源設備老舊。 缺失項目：委外廠商未定期為保養相關設備。		
影響範圍評估	將影響電腦機房之運作及相關非核心系統之線上服務之提供。		
發生原因分析	未落實監督委外廠商管理之責任。		

改善措施成效追蹤			
改善措施		**預計成效**	**執行情況**
管理面	定期進行委外廠商承辦人員之教育訓練，已落實對委外廠商之監督責任。	要求委外廠商每季進行保養，並提供相關保養紀錄。	已與委外廠商接洽。
技術面			
人力面			
資源面	更新相關電腦機房設備，並	電腦機房電源設備更新，並採用不斷電系統，於停電時可維持12小時運作。	已進行採購作業。

	確保備份設備及機制運作效果。		
作業程序			
其他			
績效管考			
改善措施確認	■合格／完成 □待追蹤(追蹤期限：____年___月___日) □不合格(說明：_____)		
經費需求或編列執行金額	○○○萬元。	經費執行情形	已進行相關電腦機房設備更新採購，共執行○○萬元。
預定完成日期	108 年 11 月 20 日	實際完成日期	108 年 11 月 20 日
完成進度或情形說明	定期檢視委外廠商之監督維護責任。		
改善成效考核			
後續成效追蹤			
資通安全推動小組	○○○	資通安全長[3]	○○○

註：陳核層級請機關依需求調整

3

12. 本校資訊系統管理與安全防護要點

國立苑裡高級中學資訊系統管理與安全防護要點

100 年 2 月 21 日行政會議通過
103 年 6 月 24 日推動資訊小組會議修正通過
104 年 10 月 08 日推動資訊小組會議修正通過
104 年 10 月 28 日國苑中圖字第 1040005434 號函核定實施
108 年 12 月 10 日推動資訊小組會議修正通過

一、目的

為強化國立苑裡高級中學（以下簡稱本校）資訊安全管理，建立安全及可信賴之電子化系統，確保資料、系統、設備及網路之安全，特依據「行政院及所屬各機關資訊安全管理要點」訂定本要點。

二、組織及權責

（一） 本校有關資訊安全管理事務依下列分工原則：

1、 資訊安全政策、計畫以及技術規範之研議、建置與評估等事項，由推動資訊小組召集人統籌資訊小組辦理。

2、 資料及資訊系統之安全需求研議、使用管理及維護等事項，由使用單位或業務承辦單位負責辦理。

3、 資訊安全之稽核作業，由政風單位會同資訊安全推動小組及相關單位負責辦理。

（二） 本校對所有行政與教學單位，每年至少進行 1 次資訊安全稽核。

（三） 本校由資訊安全推動小組負責資訊安全管理事項協調及推動。

三、人員管理及資訊安全教育訓練

（一） 各單位對資訊相關職務及工作，應進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，並進行必要之考核；各單位對可存取機密性或敏感性資訊或系統人員，及因工作需要須配賦系統存取特別權限人員，應加強評估及考核。

（二） 各單位負責重要資訊系統管理、維護、設計及操作人員，應妥適分工，分散權責，建立人力備援制度。

（三） 資訊作業相關人員離職時，應取消其進出鑰匙、磁卡及系統存取權限，並確實做好電腦軟硬體及相關文件移交工作。

（四） 各單位業務主管應負責督導所屬員工資訊作業安全，防範不法及不當行為。

（五） 資訊安全教育訓練及宣導事宜由本校資訊小組負責辦理。

四、電腦系統安全管理

（一） 各單位辦理資訊業務委外作業時，應於事前研提資訊安全需求，明訂廠商資訊安全責任及保密規定，並列入契約中，要求廠商遵守及定期考核，並派員監督。

（二） 電腦系統作業變更時，應詳實建立紀錄，以備查考。

（三） 各單位應依相關法規或契約規定，複製及使用軟體；嚴禁使用非法軟體。

（四） 電腦系統應裝置防毒軟體以防止感染電腦病毒，磁片及隨身碟使用前應事先做掃毒檢查。

（五） 使用電腦系統務必遵照本校「人員資訊安全守則」之規定。

五、網路安全管理

（一） 各單位利用網路公布及流通資訊時，除應評估資料安全等級，機密、敏感性外，未經當事人同意之個人隱私資料及文件，不得上網公布。

（二） 本校非屬機密性或敏感性資料及文件得以電子郵件或其他電子方式傳送。機密性或敏感性資料及文件，欲利用電子郵件或其他電子方式傳送時，須以適當加密或電子簽章等安全技術處理。

（三） 禁止以私人架設網路（如：行動網路、電話線等）連結機房內之主機電腦或網路設備。

六、無線網路連線控制措施

（一） 專供行政使用之無線網路熱點建議設定加密金鑰防護，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。

（二） 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。

（三） 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。

（四） 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。

（五） 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。

七、系統存取控制

（一） 各單位對電腦資料庫及檔案應建立分級（機密及安全等級）管理制度。

（二） 各項正式作業電腦系統操作及資料處理，由各權責單位指定專人負責建檔、核對、更新、審查及維護電腦資料正確性。資訊系統發展人員非經核准不得

操作使用或更改已正式作業之系統檔案。

（三） 電腦資料庫及檔案，應按不同業務範圍及使用權限，分別設定目錄、識別保護碼；重要或具機密性資料在建檔或提供使用時，應加設通行密碼、使用權限碼，以確保資料安全，且通行密碼應經常更新。

（四） 各單位離職、休職、調職人員，應立即取消使用單位內各項資源之所有權限，並列入人員離職、休職、調職之必要手續；人員職務調整及調動，應依系統存取授權規定，限期調整其權限。

（五） 各電腦系統應建立系統使用者註冊管理制度，建立使用人員名冊。

（六） 各單位重要資料及系統委外廠商處理者，不論在機關內外執行，均應採取適當及足夠安全管制措施，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

八、系統發展及維護安全管理

（一） 各單位自行開發或委外發展之系統，應在系統初始階段即將資訊安全需求納入考量；系統之維護、更新、上線執行及版本異動等作業，應予安全管制，避免不當軟體及電腦病毒危害系統安全。

（二） 對廠商軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性系統辨識碼及通行密碼；基於實際作業需要，得核發短期性及臨時性系統辨識與通行密碼供廠商使用，但使用完畢後應立即取消其使用權限。

（三） 委託廠商建置及維護重要軟硬體設施時，應在本校相關人員監督及陪同下始得為之。

九、資訊資產安全管理

（一） 各單位對於儲存各項機密資料或程式軟體之磁片、磁碟、磁帶、光碟片及報表等媒體，應設專人管理並定期備份，防止資料洩漏或損毀，並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。

（二） 對於需要長期保留或重要檔案之備份資料，應存放在防火、防潮、防磁的設備中。

（三） 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；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。

十、電腦系統實體及環境安全管理

（一） 各單位對於電腦設備裝置地點，應考量使用及管理上之安全，並應指定專人負責管理，非經奉准人員，不得隨意操作設備。管理或使用人員應詳細記載電腦設備故障、異常及維護等情形，以作為設備更新及作業安全之依據。

（二） 電腦設備機房應設置適當滅火設備。值班人員下班後，應關閉門窗及不必要電源，以確保安全。

十一、業務永續運作之規劃

若發生資訊安全事件，應立即向相關人員通報，以採取適當反應措施。若有情節嚴重者，則聯繫檢警調單位協助偵查。

十二、本要點經推動資訊小組會議通過，校長核定後公告實施。

13. 本校人員資訊安全守則

國立苑裡高級中學人員資訊安全守則

108 年 12 月 10 日推動資訊小組會議通過

1、目的：為落實國立苑裡高級中學（以下簡稱本校）資訊通訊安全作業，維護資訊及處理設備之機密性、完整性及可用性，特訂定此守則。

2、範圍：本守則適用於正職人員與約聘（僱）人員。

3、作業守則

3.1 電腦應設定密碼確實保密。

3.2 電腦應使用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為10分鐘以內。

3.3 電腦之作業系統漏洞應即時更新修補。

3.4 電腦應安裝防毒軟體並即時更新病毒碼。

3.5 應定期將重要資料備份存放。

3.6 除管理需求及經授權外，禁止使用密碼破解、網路監聽工具軟體，並不得突破他人帳號，中斷系統服務。

3.7 不得在任何公開的新聞群組、論壇、或公佈欄中透露任何有關本校資訊細節。

3.8 在丟棄任何曾經儲存本校資訊之電子媒介前，應將電子媒介中的資訊刪除，並徹底消磁或銷毀至無法解讀之程度。

3.9 敏感等級（含）以上資訊之紙本文件若不再使用時，應以碎紙機銷毀該份紙本文件，並刪除電子檔。

3.10 重要機密文件或合約，應妥善保存；若為電子檔案應考慮設定保護密碼。

3.11 開啟來路不明之電子郵件及其附件時應謹慎小心，以防電腦中毒。

3.12 當有跡象顯示系統可能中毒時，應儘速通知相關人員。

3.13 禁止濫用系統及網路資源，複製與下載非法軟體。

3.14 應遵守「電腦處理個人資料保護法」規範，保護個人資料使用之合法性及機密性。

4、密碼使用原則

4.1 應保護通行密碼，維持通行密碼的機密性；資訊系統之系統管理者至少每3 個月更換密碼一次，一般資訊系統之使用者至少每6 個月更換密碼，並禁止重複使用相同的密碼。

4.2 應避免將通行密碼記錄在書面上，或張貼於個人電腦、螢幕或其它容易洩漏秘密

之場所。

4.3 當有跡象顯示系統及通行密碼可能遭破解時，應立即更改密碼。

4.4 通行密碼的長度最少應有8 位長度，且應符合密碼設置原則。

4.5 密碼設置原則，應儘量避免使用易猜測或公開資訊為設定：

4.5.1 個人姓名、出生年月日、身分證字號。

4.5.2 機關或單位名稱識別代碼或是其他相關事項。

4.5.3 使用者識別碼、使用者姓名、群體使用者之識別碼或是其他系統識別碼。

4.5.4 電腦主機名稱、作業系統名稱、或電腦上使用者的名稱。

4.5.5 電話號碼。

4.5.6 英文或是其他外文字典的字彙。

4.5.7 專有名詞。

4.5.8 空白。

4.6 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。

4.7 資訊系統與服務應避免使用共用帳號及通行碼。

5、電腦軟體版權之使用與管理

5.1 禁止使用未經授權之電腦軟體，遵守智慧財產權相關規定。

5.2 本校資訊機房伺服器所使用之電腦軟體均須具有合法版權，人員不得私自安裝非法電腦軟體。

5.3 本校人員若有安裝機房伺服器軟體需求時，需填寫「資訊服務申請表」，經權責主管以上核准後，始得執行安裝。

6、保密協定

6.1 本校人員應填具「保密切結書」，承諾任職期間，因職務上所獲悉之任何資訊或持有之資料、檔案、技術、財務或業務上之機密，非經主管授權不得對外透露或加以濫用。

7、公告與實施

7.1 本守則由本校推動資訊小組會議通過，校長核定後公告實施。

7.2 本校員工若未遵守上述規定或資訊安全政策及程序者，得依相關懲戒程序處置違紀人員。