資通安全維護計畫範本參考附件

目　次

1. 資通安全推動小組成員及分工表

國立屏北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01月29日

單位職級	名稱	職掌事項	分機	備註 （代理人）
資通安全長	本校校長	1. 資訊安全長擔任本小組之召集人，召集相關單位召開會議，制訂或修正本校資安政策 2. 跨部門資通安全事項權責分工之協調 3. 整體資通安全措施之協調 4. 資通安全計畫之協調	511	依據本校校長代理順序
資安執行秘書	圖書館主任	1. 協助資訊安全長制訂、修正及執行資安政策 2. 研議整體資通安全措施 3. 研議資通安全計畫 4. 研議應採用之資通安全技術、方法及程序 5. 研議其他重要資通安全事項	560	資安第一聯絡人 第一代理為總務主任
諮詢委員	外聘專家學者	藉助業界或學界專業人力，提供諮詢意見，以協助各項資安政策與計畫之擬定		
策略規劃組	圖書館主任 教務主任 學務主任 輔導主任 總務主任	1. 研議資通安全政策及目標 2. 訂定機關資通安全相關規章與程序、制度文件，並確保相關規章與程序、制度合乎法令及契約之要求 3. 依據資通安全目標擬定機	560 520 530 550 540	

		關年度工作計畫 4. 傳達機關資通安全政策與目標 5. 其他資通安全事項之規劃		
資安防護組	網管協辦 委外網路維護工程師 設備組組長 輔導主任 庶務組組長 文書組組長 出納組組長 註冊組幹事 訓育組幹事	1. 資通安全技術之研究、建置及評估相關事項。 2. 資通安全相關規章與程序、制度之執行。 3. 資訊及資通系統之盤點及風險評估。 4. 資料及資通系統之安全防護事項之執行。 5. 資通安全事件之通報及應變機制之執行。 6. 其他資通安全事項之辦理與推動。	561 523 550 541 542 543 522 534	
績效管理組	主任秘書 主計主任 人事主任	1. 辦理資通安全內部稽核。 2. 每年定期召開資通安全管理審查會議，提報資通安全事項執行情形。	511 580 570	

資通安全長：

2. 資通安全保密同意書

國立屏北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

國立屏北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01月29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	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	

4. 管制區域人員進出登記表

國立屏北高級中學管制區域人員進出登記表

編號：○○

製表日期：108年01月29日

編號	姓名	單位	配同人員	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：　　單位主管：

5. 委外廠商執行人員保密切結書、保密同意書

國立屏北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）委派至國立屏北高級中學（以下稱本校）處理業務，謹聲明恪遵本校下列工作規定，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，非經本校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，不得私自將本校之資訊設備、媒體檔案及公務文書攜出。

二、 未經本校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本校網路。若經申請獲准連接本校網路，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本校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本校配發之個人電腦與週邊設備，並僅開放使用本校內部網路。若因業務需要使用本校電子郵件、目錄服務，應經本校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本校業務相關人員之確認並代為申請核准。

五、 本校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（以授課時需連結本校網路者為限）及經常到本校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本校洽公之業務人員每年簽署本切結書乙次。

中　華　民　國　　年　　月　　日

國立屏北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）得標國立屏北高級中學（以下稱本校）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本校未標示得對外公開之公務秘密，以及本校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，於本校指定之處所內使用之。非經本校事前書面同意，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，亦不得攜至本校或本校所指定處所以外之處所。

第二條　簽署人知悉或取得本校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，由本校提供以前，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、依契約本校業已不負保密責任、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，本校得請求簽署人及其任職之廠商賠償本校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，本校、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

國立屏北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。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	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。
	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。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	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。
	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	3. 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。
	4. 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. 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	1. 是否定期辦理資通安全認知宣導？	■	□	□	有定期辦理宣導。
	2. 是否對同仁進行資安評量？	■	□	□	按期進行資安評量。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
及教育訓練	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。
	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。
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	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。
	2. 是否追蹤過去缺失之改善情形？	■	□	□	有追蹤缺失改善之情形。
	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。

單位主管：　　資通安全長：

7. 年度資通安全教育訓練計畫

國立屏北高級中學108年度資通安全教育訓練計畫

壹、依據

國立屏北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校之資通安全維護計畫，以強化本校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

本機關所屬人員：

人員類別	人數
資通安全專責人員	1
一般人員	25
主管人員	7
共計	○○

肆、訓練項目（各機關自行定義）

人員類別	訓練課程[1]	時數
資通安全專責人員	電子郵件安全 ○○	12小時
主管人員、資訊人員及一般人員	資訊安全通識及本校資通安全維護計畫	3小時

伍、訓練期程

[1]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

預計於108年12月行政會議後舉行3小時的資安教育訓練。

陸、訓練方式

以實體課程方式，邀請講師說明本校資通安全維護計畫及資通安全通識。

8. 資通安全認知宣導及教育訓練簽到表

國立屏北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：資訊安全通識及本校資通安全維護計畫

時　　間：108年 12 月　　日 9：10－11：00

地　點：＿＿本校行政大樓三樓會議室＿＿＿＿＿＿＿＿＿＿

單 位	職 稱	姓 名	簽 名
人事室	專員	○○○	

9. 資通安全維護計畫實施情形

國立屏北高級中學資通安全維護計畫實施情形

編號：○○

本機關(單位)之業務因涉及全國性民眾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Ｃ級，依資通安全管理法第12條之規定，向 鈞部（院）提出本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
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	本機關已指定校長為資通安全長，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四人，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	5.1 資訊及資通系統之盤點	本機關已於今年○月盤點本機關之資

之盤點及核心資通系統、相關資產之標示		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C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1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	1. 資通安全防護及控制措施	本機關已依依安全維護計畫辦理，詳附件資料。(導入 CNS27001機關)
	7.1 資訊及通系統之保管	本機關已依依安全維護計畫辦理，詳附件資料。(以下為未導入 CNS27001機關之範例)
	7.2 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。
	7.3 作業及通訊安全管理	本機關已依依安全維護計畫辦理。
	7.4 系統獲取、開發及維護	本機關已依依安全維護計畫辦理。
	7.5 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。
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○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資通安全事項之考核機制	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。
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		

單位主管：　　資通安全長：

10. 資通安全稽核計畫

國立屏北高級中學108年度資通安全稽核計畫

壹、依據

一、國立屏北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

為瞭解本校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

由各機關自行排定稽核期程。

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

適用範圍涵蓋國立屏北高級中學全機關

陸、稽核項目及內容

一、核心業務及其重要性：本機關之核心業務及重要性如下表：

核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
校務行政	校務行政系統	■為本機關依組織法執掌，足認為重要者	無法即時更新校務行政資訊，但仍可手動作業，短時間內不影響校務行政運作。	48小時

學生學習歷程	學生學習歷程系統	■為本機關依組織法執掌，足認為重要者	學生無法上傳個人學習歷程資料，授課老師無法認證課程學習成果，但因可上傳資料的期程較長，系統中斷的容忍度較高	72小時
學校官網	學校網頁	■為本機關依組織法執掌，足認為重要者	影響學校資訊佈達的方便性及時效性，但仍可以校內廣播、文件或電話方式通知重要訊息，不會造成重大影響。	48小時
網路轉址服務	DNS	■為本機關依組織法執掌，足認為重要者	可能導致僅能以 IP 方式存取學校網路資源，造成民眾和學生使用不便，以及電子郵件系統無法收送信件(本校採 g suite 服務)，雖然會造成通訊上的不便，但不影響學校校務正常運作	48小時

二、資通安全政策及目標：

(一)、 資通安全政策

為使本機關業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性（Confidentiality）、完整性（Integrity）及可用性（Availability），特制訂本政策如下，以供全體同仁共同遵循：

應建立資通安全風險管理機制，定期因應內外在資通安全情勢變化，檢討資通安全風險管理之有效性。

1. 應保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。

2. 應強固核心資通系統之韌性，確保機關業務持續營運。

3. 應因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本校同仁之資通安全意識，本機關同仁亦應確實參與訓練。

4. 針對辦理資通安全業務有功人員應進行獎勵。

5. 勿開啟來路不明或無法明確辨識寄件人之電子郵件。

6. 禁止多人共用單一資通系統帳號。

(二)、 資通安全目標

1. 量化型目標

(1) 核心資通系統可用性達95%以上。(中斷時數/總運作時數≤ 5%)(確保本校關鍵業務系統資訊機房維運服務達全年上班時間95%以上可用性，並確保：因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每年不得超過12次，且每次不超過72工作小時。)

(2) 知悉資安事件發生，能於規定的時間完成通報、應變及復原作業。

2. 質化型目標：

適時因應法令與技術之變動，調整資通安全維護之內容，以避免資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。

(1) 達成資通安全責任等級分級之要求，並降低遭受資通安全風險威脅。

(2) 提升人員資安防護意識、有效偵測與預防外部攻擊等。

三、資通安全推動組織：(內容由各機關自行定義)

(三)、 資通安全推動小組

1. 組織

為推動本機關之資通安全相關政策、落實資通安全事件通報及相關應變處理，由資通安全長召集各處室主任/組長以上之人員代表成立資通安全推動小組，其任務包括：

(1) 跨部門資通安全事項權責分工之協調。

(2) 應採用之資通安全技術、方法及程序之協調研議。

(3) 整體資通安全措施之協調研議。

(4) 資通安全計畫之協調研議。

(5) 其他重要資通安全事項之協調研議。

2. 分工及職掌

本機關之資通安全推動小組依下列分工進行責任分組，並依資通安全長之指示負責下列事項，本機關資通安全推動小組分組人員名單及職掌應列冊，並適時更新之：

(1) 策略規劃組：

- 資通安全政策及目標之研議。
- 訂定機關資通安全相關規章與程序、制度文件，並確保相關規章與程序、制度合乎法令及契約之要求。
- 依據資通安全目標擬定機關年度工作計畫。
- 傳達機關資通安全政策與目標。
- 其他資通安全事項之規劃。

(2) 資安防護組：

- 資通安全技術之研究、建置及評估相關事項。
- 資通安全相關規章與程序、制度之執行。
- 資訊及資通系統之盤點及風險評估。
- 資料及資通系統之安全防護事項之執行。
- 資通安全事件之通報及應變機制之執行。
- 其他資通安全事項之辦理與推動。

(3) 績效管理組：

- 辦理資通安全內部稽核。
- 每年定期召開資通安全管理審查會議，提報資通安全事項執行情形。

四、專責人力及經費之配置：

(四)、 專責人力及資源之配置

本機關依資通安全責任等級分級辦法之規定，屬資通安全責任等級 C 級，

最低應設置資通安全專責人員1人，其分工如下，本機關現有資通安全專責人員名單及職掌應列冊，並適時更新。

1. 資通安全管理面業務1人，負責推動資通系統防護需求分級、資通安全管理系統導入及驗證、內部資通安全稽核、機關資安治理成熟度評估及教育訓練等業務之推動。

2. 資通系統安全管理業務1人，負責資通系統分級及防護基準、安全性檢測、業務持續運作演練等業務之推動。

3. 資通安全防護業務1人，負責資通安全監控管理機制、政府組態基準導入，資通安全防護設施建置及資通安全事件通報及應變業務之推動。

4. 資通安全管理法法遵事項業務1人，負責本機關對所屬公務務機關或所管特定非公務機關之法遵義務執行事宜。

本機關之承辦單位於辦理資通安全人力資源業務時，應加強資通安全人員之培訓，並提升機關內資通安全專業人員之資通安全管理能力。本機關之相關單位於辦理資通安全業務時，如資通安全人力或經驗不足，得洽請相關學者專家或專業機關（構）提供顧問諮詢服務。

資安專責人員專業職能之培養(如證書、證照、培訓紀錄等)，應依據資通安全責任等級分級辦法之規定。

1. 資安專責人員總計應持有1張以上資通安全專業證照。

2. 資安專責人員總計應持有1張以上資通安全職能評量證書。

本機關負責重要資通系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，若負有機密維護責任者，應簽屬書面約定，並視需要實施人員輪調，建立人力備援制度。

本機關之首長及各級業務主管人員，應負責督導所屬人員之資通安全作業，防範不法及不當行為。

專業人力資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

(五)、 經費之配置

1. 資通安全推動小組於規劃配置相關經費及資源時，應考量本機關之資通安全政策及目標，並提供建立、實行、維持及持續改善資通安全維護計畫所需之資源。

2. 各單位於規劃建置資通系統建置時，應一併規劃資通系統之資安防護需求，並於整體預算中合理分配資通安全預算所佔之比例。

3. 各單位如有資通安全資源之需求，應配合機關預算規劃期程向資通安全推動小組提出，由資通安全推動小組視整體資通安全資源進行分配，並經資通安全長核定後，進行相關之建置。

4. 資通安全經費、資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

五、公務機關資通安全長之配置：

依本法第11條之規定，本校訂定校長為資通安全長，負責督導機關資通安全相關事項，其任務包括：

資通安全管理政策及目標之核定、核轉及督導。

1. 資通安全責任之分配及協調。

2. 資通安全資源分配。

3. 資通安全防護措施之監督。

4. 資通安全事件之檢討及監督。

5. 資通安全相關規章與程序、制度文件核定。

6. 資通安全管理年度工作計畫之核定

7. 資通安全相關工作事項督導及績效管理。

8. 其他資通安全事項之核定。

六、資訊及資通系統之盤點，並標示核心資通系統及相關資產：

(六)、 **資訊及資通系統盤點**

- 本機關每年辦理資訊及資通系統資產盤點，依管理責任指定對應之資產管理人，並依資產屬性進行分類，分別為資訊資產、軟體資產、實體資產、支援服務資產等。

1. 資訊及資通系統資產項目如下：

- 資訊資產：以數位等形式儲存之資訊，如資料庫、資料檔案、系統文件、操作手冊、訓練教材、研究報告、作業程序、永續運作計畫、

稽核紀錄及歸檔之資訊等。

(1) 軟體資產：應用軟體、系統軟體、開發工具、套裝軟體及電腦作業系統等。

(2) 實體資產：電腦及通訊設備、可攜式設備及資通系統相關之設備等。

(3) 支援服務資產：相關基礎設施級其他機關內部之支援服務，如電力、消防等。

2. 本機關每年度應依資訊及資通系統盤點結果，製作「資訊及資通系統資產清冊」，欄位應包含：資訊及資通系統名稱、資產名稱、資產類別、擁有者、管理者、使用者、存放位置、防護需求等級。

3. 資訊及資通系統資產應以標籤標示於設備明顯處，並載明財產編號、保管人、廠牌、型號等資訊。核心資通系統及相關資產，並應加註標示。

4. 各單位管理之資訊或資通系統如有異動，應即時通知資通安全推動小組更新資產清冊。

(七)、 機關資通安全責任等級分級

本機關自行維運資通系統，為資通安全等級分類Ｃ級機關。

(八)、 資通安全風險評估

本機關應每年針對資訊及資通系統資產進行風險評估。

1. 執行風險評估時應參考行政院國家資通安全會報頒布之最新「資訊系統風險評鑑參考指引」，並依其中之「詳細風險評鑑方法」進行風險評估之工作。

2. 本機關應每年依據資通安全責任等級分級辦法之規定，分別就機密性、完整性、可用性、法律遵循性等構面評估自行或委外開發之資通系統防護需求分級。

(九)、 核心資通系統及最大可容忍中斷時間

核心資通系統	資訊資產	最大可容忍中斷時間	核心資通系統主要功能

校務行政系統	1.機架型伺服器1台 2.資料庫管理系統1套 3.整合式多功能防火牆 FortiGate 101E 4.網路交換器(ZYXEL XS3700-24)	48小時	1.提供教職員輸入及輸出學籍、成績及缺曠資料 2.提供學生及家長查詢成績及缺曠服務
學生學習歷程系統	1.機架型伺服器1台 2.資料庫管理系統1套 3.整合式多功能防火牆 FortiGate 101E 4.網路交換器(ZYXEL XS3700-24)	72小時	1.提供學生上傳個人學習歷程資料 2.提供授課教師進行學習成果認證
學校網站系統	1.機架型伺服器1台 2.客製化網站套件1組 3.整合式多功能防火牆 FortiGate 101E 4.網路交換器(ZYXEL XS3700-24)	48小時	1.提供本校相關資訊予親師生及民眾 2.本校各項資訊服務的入口網站
DNS	1.機架型伺服器1台 2.整合式多功能防火牆 FortiGate 101E 3.網路交換器(ZYXEL XS3700-24)	48小時	IP與網域名稱轉換

七、資通安全防護及控制措施：

本機關依據前章資通安全風險評估結果、自身資通安全責任等級之應辦事項及核心資通系統之防護基準，採行相關之防護及控制措施。

本機關依據前章資通安全風險評估結果、自身資通安全責任等級之應辦事項及核心資通系統之防護基準，採行相關之防護及控制措施如下:

(十)、 資訊及資通系統之管理

1. 資訊及資通系統之保管

(1) 資訊及資通系統管理人應確保資訊及資通系統已盤點造冊並適切分級，並持續更新以確保其正確性。

(2) 資訊及資通系統管理人應確保資訊及資通系統被妥善的保存或備份。

(3) 資訊及資通系統管理人應確保重要之資訊及資通系統已採取適當之存取控制政策。

2. 資訊及資通系統之使用

(1) 本機關同仁使用資訊及資通系統前應經其管理人授權。

(2) 本機關同仁使用資訊及資通系統時，應留意其資通安全要求事項，並負對應之責任。

(3) 本機關同仁使用資訊及資通系統後，應依規定之程序歸還。資訊類資訊之歸還應確保相關資訊已正確移轉，並安全地自原設備上抹除。

(4) 非本機關同仁使用本機關之資訊及資通系統，應確實遵守本機關之相關資通安全要求，且未經授權不得任意複製資訊。

(5) 對於資訊及資通系統，宜識別並以文件記錄及實作可被接受使用之規則。

3. 資訊及資通系統之刪除或汰除

(1) 資訊及資通系統之刪除或汰除前應評估機關是否已無需使用該等資訊及資通系統，或該等資訊及資通系統是否已妥善移轉或備份。

(2) 資訊及資通系統之刪除或汰除時宜加以清查，以確保所有機敏性資訊及具使用授權軟體已被移除或安全覆寫。

(3) 具機敏性之資訊或具授權軟體之資通系統，宜採取實體銷毀，或以毀損、刪除或覆寫之技術，使原始資訊無法被讀取，並避免僅使用標準刪除或格式化功能。

(十一)、 存取控制與加密機制管理

1. 網路安全控管：

本機關之網路區域劃分如下：

- 外部網路：對外網路區域，連接外部廣網路。
- 非軍事區(DMZ)：放置機關對外服務伺服器之區段。

- 內部區域網路 (Local Area Network, LAN) ：機關內部單位人員及內部伺服器使用之網路區段。

(1) 外部網路、非軍事區及內部區域網路間連線需經防火牆進行存取控制，非允許的服務與來源不能進入其他區域。

(2) 應定期檢視防火牆政策是否適當，並適時進行防火牆軟、硬體之必要更新或升級。

(3) 對於通過防火牆之來源端主機 IP 位址、目的端主機 IP 位址、來源通訊埠編號、目的地通訊埠編號、通訊協定、登入登出時間、存取時間以及採取的行動，均應予確實記錄。

(4) 本機關內部網路之區域應做合理之區隔，使用者應經授權後在授權之範圍內存取網路資源。

(5) 對網路系統管理人員或資通安全主管人員的操作，均應建立詳細的紀錄。並應定期檢視網路安全相關設備設定規則與其日誌紀錄，並檢討執行情形。

(6) 使用者應依規定之方式存取網路服務，不得於辦公室內私裝電腦及網路通訊等相關設備。

(7) 網域名稱系統(DNS)防護

- 一般伺服器應關閉 DNS 服務，防火牆政策亦應針對 DNS 進行控管，關閉不需要的 DNS 服務存取。
- DNS 伺服器應經常性進行弱點漏洞管理與修補、落實存取管控機制。
- DNS 伺服器應設定指向 GSN Cache DNS。
- 本校內部主機位置查詢應指向本校 DNS 伺服器。

(8) 無線網路防護

- 機密資料原則不得透過無線網路及設備存取、處理或傳送。
- 無線設備應具備安全防護機制以降低阻斷式攻擊風險，且無線網路之安全防護機制應包含外來威脅及預防內部潛在干擾。
- 行動通訊或紅外線傳輸等無線設備原則不得攜入涉及或處理機密資料之區域。
- 用以儲存或傳輸資料且具無線傳輸功能之個人電子設備與工作

站，應安裝防毒軟體，並定期更新病毒碼。

2. 資通系統權限管理

(1) 本機關之資通系統應設置通行碼管理，通行碼之要求需滿足：

- 通行碼長度8碼以上。
- 通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以上。
- 使用者每90天應更換一次通行碼。

(2) 使用者使用資通系統前應經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要經核准並紀錄外，不得共用 ID。

(3) 使用者無繼續使用資通系統時，應立即停用或移除使用者 ID，資通系統管理者應定期清查使用者之權限。

3. 特權帳號之存取管理

(1) 資通系統之特權帳號請應經正式申請授權方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。

(2) 資通系統之特權帳號不得共用。

(3) 對於特權帳號，宜指派與該使用者日常公務使用之不同使用者 ID。

(4) 資通系統之特權帳號應妥善管理，並應留存特殊權限帳號之使用軌跡。

(5) 資通系統之管理者每季應清查系統特權帳號並劃定特權帳號逾期之處理方式。

4. 加密管理

本機關之機密資訊於儲存或傳輸時應進行加密。本機關之加密保護措施應遵守下列規定：

(1) 應落實使用者更新加密裝置並備份金鑰。

(2) 應避免留存解密資訊。

(3) 一旦加密資訊具遭破解跡象，應立即更改之。

(十二)、 作業與通訊安全管理

1. 防範惡意軟體之控制措施

(1) 本機關之主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。

經任何形式之儲存媒體所取得之檔案，於使用前應先掃描有無惡意軟體。

- 電子郵件附件及下載檔案於使用前，宜於他處先掃描有無惡意軟體。
- 確實執行網頁惡意軟體掃描。

(2) 使用者未經同意不得私自安裝應用軟體，管理者並應每半年定期針對管理之設備進行軟體清查。

(3) 使用者不得私自使用已知或有嫌疑惡意之網站。

(4) 設備管理者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊。

2. 遠距工作之安全措施

(1) 本機關資通系統之操作及維護以現場操作為原則，避免使用遠距工作，如有緊急需求時，應申請並經資通安全推動小組同意後始可開通。

(2) 資通安全推動小組應定期審查已授權之遠距工作需求是否適當。

(3) 針對遠距工作之連線應採適當之防護措施(並包含伺服器端之集中過濾機制檢查使用者之授權)，並且記錄其登入情形。

- 提供適當通訊設備，並指定遠端存取之方式。
- 提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。
- 進行遠距工作時之安全監視。
- 遠距工作終止時之存取權限撤銷，並應返還相關設備。

3. 電子郵件安全管理

(1) 本機關人員到職後應經申請方可使用電子郵件帳號，並應於人員離職後刪除電子郵件帳號之使用。

(2) 電子郵件系統管理人應定期進行電子郵件帳號清查。

(3) 電子郵件伺服器應設置防毒及過濾機制，並適時進行軟硬體之必要更新。

(4) 使用者使用電子郵件時應提高警覺，並使用純文字模式瀏覽，避免讀取來歷不明之郵件或含有巨集檔案之郵件。

(5) 原則不得電子郵件傳送機密性或敏感性之資料，如有業務需求者應依相關規定進行加密或其他之防護措施。

(6) 使用者不得利用機關所提供電子郵件服務從事侵害他人權益或違法之行為。

(7) 使用者應確保電子郵件傳送時之傳遞正確性。

(8) 使用者使用電子郵件時，應注意電子簽章之要求事項。

(9) 本機關應定期舉辦(或配合上級機關舉辦)電子郵件社交工程演練，並檢討執行情形。

4. 確保實體與環境安全措施

(1) 資料中心及電腦機房之門禁管理

- 資料中心及電腦機房應進行實體隔離。
- 機關人員或來訪人員應申請及授權後方可進入資料中心及電腦機房，資料中心及電腦機房管理者並應定期檢視授權人員之名單。
- 人員進入管制區應配載身分識別之標示，並隨時注意身分不明或可疑人員。
- 僅於必要時，得准許外部支援人員進入資料中心及電腦機房。
- 人員及設備進出資料中心及電腦機房應留存記錄。

(2) 資料中心及電腦機房之環境控制

- 資料中心及電腦機房之空調、電力應建立備援措施。
- 資料中心及電腦機房之溫濕度管控範圍為：
- 資料中心及電腦機房應安裝之安全偵測及防護措施，包括熱度及煙霧偵測設備、火災警報設備、溫濕度監控設備、漏水偵測設備、入侵者偵測系統，以減少環境不安全引發之危險。
- 各項安全設備應定期執行檢查、維修，並應定時針對設備之管理者進行適當之安全設備使用訓練。

(3) 辦公室區域之實體與環境安全措施

- 應考量採用辦公桌面的淨空政策，以減少文件及可移除式媒體等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。
- 文件及可移除式媒體在不使用或不上班時，應存放在櫃子內。
- 機密性及敏感性資訊，不使用或下班時應該上鎖。
- 機密資訊或處理機密資訊之資通系統應避免存放或設置於公眾可接觸之場域。
- 顯示存放機密資訊或具處理機密資訊之資通系統地點之通訊錄及內部人員電話簿，不宜讓未經授權者輕易取得。
- 資訊或資通系統相關設備，未經管理人授權，不得被帶離辦公室。

5. 資料備份

(1) 重要資料及核心資通系統應進行資料備份，其備份之頻率應滿足復原時間點目標之要求，並執行異地存放。

(2) 本機關應每季確認核心資通系統資料備份之有效性。且測試該等資料備份時，宜於專屬之測試系統上執行，而非直接於覆寫回原資通系統。

(3) 敏感或機密性資訊之備份應加密保護。

6. 媒體防護措施

(1) 使用隨身碟或磁片等存放資料時，具機密性、敏感性之資料應與一般資料分開儲存，不得混用並妥善保管。

(2) 資訊如以實體儲存媒體方式傳送，應留意實體儲存媒體之包裝，選擇適當人員進行傳送，並應保留傳送及簽收之記錄。

(3) 為降低媒體劣化之風險，宜於所儲存資訊因相關原因而無法讀取前，將其傳送至其他媒體。

(4) 對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感之紙本或備份磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙。

7. 電腦使用之安全管理

(1) 電腦、業務系統或自然人憑證，若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。

(2) 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。

(3) 連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

(4) 筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

(5) 下班時應關閉電腦及螢幕電源。

(6) 如發現資安問題，應主動循機關之通報程序通報。

(7) 支援資訊作業的相關設施如影印機、傳真機等，應安置在適當地點，以降低未經授權之人員進入管制區的風險，及減少敏感性資訊遭破解或洩漏之機會。

8. 行動設備之安全管理

(1) 機密資料不得由未經許可之行動設備存取、處理或傳送。

(2) 機敏會議或場所不得攜帶未經許可之行動設備進入

9. 即時通訊軟體之安全管理

(1) 使用即時通訊軟體傳遞機關內部公務訊息，其內容不得涉及機密資料。但有業務需求者，應使用經專責機關鑑定相符機密等級保密機制或指定之軟、硬體，並依相關規定辦理。

(2) 使用於傳遞公務訊息之即時通訊軟體應具備下列安全性需求：

- 用戶端應有身分識別及認證機制。
- 訊息於傳輸過程應有安全加密機制。
- 應通過經濟部工業局訂定行動化應用軟體之中級檢測項目。
- 伺服器端之主機設備及通訊紀錄應置於我國境內。
- 伺服器通訊紀錄（log）應至少保存六個月。

(十三)、 系統獲取、開發及維護

本機關之資通系統應依「資通安全責任等級分級辦法」附表九之規定完成系統防護需求分級，依分級之結果，完成附表十中資通系統防護基準，並注意下列事項：

1. 開發過程請依安全系統發展生命週期(Secure Software Development Life Cycle, SSDLC)納入資安要求，並參考行政院國家資通安全會報頒布之最新「安全軟體發展流程指引」、「安全軟體設計指引」及

「安全軟體測試指引」。

2. 於資通系統開發前，設計安全性要求，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾，並檢討執行情形。

3. 於上線前執行安全性要求測試，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試，並檢討執行情形。

4. 執行資通系統源碼安全措施，包含源碼存取控制與版本控管，並檢討執行情形。

(十四)、 **業務持續運作演練**

本機關應針對核心資通系統制定業務持續運作計畫，並每二年辦理一次核心資通系統持續運作演練。

(十五)、 **執行資通安全健診**

本機關每二年應辦理資通安全健診，其至少應包含下列項目，並檢討執行情形：

1. 網路架構檢視。

2. 網路惡意活動檢視。

3. 使用者端電腦惡意活動檢視。

4. 伺服器主機惡意活動檢視。

5. 安全設定檢視。

(十六)、 **資通安全防護設備**

1. 本機關應建置防毒軟體、網路防火牆、電子郵件過濾裝置，持續使用並適時進行軟、硬體之必要更新或升級。

2. 資安設備應定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形。

八、資通安全事件通報、應變及演練相關機制：

為即時掌控資通安全事件，並有效降低其所造成之損害，本機關訂有資通安全事件通報、應變及演練相關機制，詳資通安全事件通報應變程

序。

九、資通安全情資之評估及因應機制：

本機關接獲資通安全情資，應評估該情資之內容，並視其對本機關之影響、本機關可接受之風險及本機關之資源，決定最適當之因應方式，必要時得調整資通安全維護計畫之控制措施，並做成紀錄。

(十七)、 資通安全情資之分類評估

本機關接受資通安全情資後，應指定資通安全專職人員進行情資分析，並依據情資之性質進行分類及評估，情資分類評估如下：

1. 資通安全相關之訊息情資

資通安全情資之內容如包括重大威脅指標情資、資安威脅漏洞與攻擊手法情資、重大資安事件分析報告、資安相關技術或議題之經驗分享、疑似存在系統弱點或可疑程式等內容，屬資通安全相關之訊息情資。

2. 入侵攻擊情資

資通安全情資之內容如包含特定網頁遭受攻擊且證據明確、特定網頁內容不當且證據明確、特定網頁發生個資外洩且證據明確、特定系統遭受入侵且證據明確、特定系統進行網路攻擊活動且證據明確等內容，屬入侵攻擊情資。

3. 機敏性之情資

資通安全情資之內容如包含姓名、出生年月日、國民身份證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病例、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接識別之個人資料，或涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或情資之公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益，或涉及一般公務機密、敏感資訊或國家機密等內容，屬機敏性之情資。

4. 涉及核心業務、核心資通系統之情資

資通安全情資之內容如包含機關內部之核心業務資訊、核心資通系統、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作等內容，屬涉及核心業務、核心資通系統之情資。

(十八)、 資通安全情資之因應措施

本機關於進行資通安全情資分類評估後，應針對情資之性質進行相應之措施，必要時得調整資通安全維護計畫之控制措施。

1. 資通安全相關之訊息情資

由資通安全推動小組彙整情資後進行風險評估，並依據資通安全維護計畫之控制措施採行相應之風險預防機制。

2. 入侵攻擊情資

由資通安全專職(責)人員判斷有無立即之危險，必要時採取立即之通報應變措施，並依據資通安全維護計畫採行相應之風險防護措施，另通知各單位進行相關之預防。

3. 機敏性之情資

就涉及個人資料、營業秘密、一般公務機密、敏感資訊或國家機密之內容，應採取遮蔽或刪除之方式排除，例如個人資料及營業秘密，應以遮蔽或刪除該特定區段或文字，或採取去識別化之方式排除之。

4. 涉及核心業務、核心資通系統之情資

資通安全推動小組應就涉及核心業務、核心資通系統之情資評估其是否對於機關之運作產生影響，並依據資通安全維護計畫採行相應之風險管理機制。

十、資通系統或服務委外辦理之管理措施：

本機關委外辦理資通系統之建置、維運或資通服務之提供時，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

(十九)、 選任受託者應注意事項

(1) 受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。

1. 受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

2. 受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之

受託者應具備之資通安全維護措施。

(二十)、 監督受託者資通安全維護情形應注意事項

受託業務包括客製化資通系統開發者，受託者應提供該資通系統之第三方安全性檢測證明；涉及利用非自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

1. 受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。
2. 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行委託契約而持有之資料。
3. 受託者應採取之其他資通安全相關維護措施。
4. 本機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

十一、公務機關所屬人員辦理業務涉及資通安全事項之考核機制：

本機關所屬人員之平時考核或聘用，依據公務機關所屬人員資通安全事項獎懲辦法、公立高級中等以下學校教師成績考核辦法、公務人員考績法施行細則、國立屏北高級中學學生獎懲規定，及本機關各相關規定辦理之。

十二、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：

(二十一)、 資通安全維護計畫之實施

為落實本安全維護計畫，使本機關之資通安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時，應與本機關之資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。

(二十二)、 資通安全維護計畫實施情形之稽核機制

1. 稽核機制之實施

(1) 資通安全推動小組應定期(至少每年一次)或於系統重大變更或組織改造後執行一次內部稽核作業，以確認人員是否遵循本規範與機關之管理程序要求，並有效實作及維持管理制度。

(2) 辦理稽核前資通安全推動小組應擬定資通安全稽核計畫，並安排稽核成員，稽核計畫應包括稽核之依據與目的、期間、重點領域、稽核小組組成方式、保密義務、稽核方式、基準與項目及受稽單位協助事項，並應將前次稽核之結果納入稽核範圍。

(3) 辦理稽核時，資通安全推動小組應於執行稽核前○○日，通知受稽核單位，並將稽核期程、稽核項目紀錄表及稽核流程等相關資訊提供受稽單位。

(4) 本機關之稽核人員應受適當培訓並具備稽核能力，且不得稽核自身經辦業務，以確保稽核過程之客觀性及公平性；另，於執行稽核時，應填具稽核項目紀錄表，待稽核結束後，應將稽核項目紀錄表內容彙整至稽核結果及改善報告中，並提供給受稽單位填寫辦理情形。

(5) 稽核結果應對相關管理階層(含資安長)報告，並留存稽核過程之相關紀錄以作為資通安全稽核計畫及稽核事件之證據。

(6) 稽核人員於執行稽核時，應至少執行一項特定之稽核項目（如是否瞭解資通安全政策及應負之資安責任、是否訂定人員之資通安全作業程序與權責、是否定期更改密碼）。

2. 稽核改善報告

(1) 受稽單位於稽核實施後發現有缺失或待改善項目者，應對缺失或待改善之項目研議改善措施、改善進度規劃，並落實執行。

(2) 受稽單位於稽核實施後發現有缺失或待改善者，應判定其發生之原因，並評估是否有其類似之缺失或待改善之項目存在。

(3) 受稽單位於判定缺失或待改善之原因後，應據此提出並執行相關之改善措施及改善進度規劃，必要時得考量對現行資通安全管理制度或相關文件進行變更。

(4) 機關應定期審查受稽單位缺失或待改善項目所採取之改善措施、改善進度規劃及佐證資料之有效性。

(5) 受稽單位於執行改善措施時，應留存相關之執行紀錄，並填寫稽核結果及改善報告。

(二十三)、 資通安全維護計畫之持續精進及績效管理

1. 本機關之資通安全推動小組應於一月份(每年至少一次)召開資通安全

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。

2. 管理審查議題應包含下列討論事項：

(1) 過往管理審查議案之處理狀態。

(2) 與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資通安全推動小組決議事項等。

(3) 資通安全維護計畫內容之適切性。

(4) 資通安全績效之回饋，包括：

- 資通安全政策及目標之實施情形。
- 資通安全人力及資源之配置之實施情形。
- 資通安全防護及控制措施之實施情形。
- 內外部稽核結果。
- 不符合項目及矯正措施。

(5) 風險評鑑結果及風險處理計畫執行進度。

(6) 重大資通安全事件之處理及改善情形。

(7) 利害關係人之回饋。

(8) 持續改善之機會。

3. 持續改善機制之管理審查應做成改善績效追蹤報告，相關紀錄並應予保存，以作為管理審查執行之證據。

柒、改善作業

自行評估對於稽核結果表現優良者是否給予行政獎勵，並針對缺失或待改善項目者研擬後續追蹤方式及頻率(如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. 稽核項目紀錄表

國立屏北高級中學稽核項目紀錄表

稽核日期： 108 年　　月　　日

稽核範圍：全機關

受稽核單位	稽核項目	稽核結果	備註
EX：總務處	資產盤點	■符合 □不符合 □不適用	經驗證其資產項目表，按規定進行資產盤點，各項資產均依規定建檔並指派責任人。
EX：人事室	權限控管	□符合 ■不符合 □不適用	可使用高權限登入 A 網站，提供一般同仁進行課程報到作業外，亦可查詢所有同仁之個人資料。
		■符合 □不符合 □不適用	
		■符合 □不符合 □不適用	
		■符合 □不符合 □不適用	
		■符合 □不符合 □不適用	
附註			
受稽核人員：王○○			受稽核單位主管：黃○○

註：陳核層級請機關依需求調整

12. 稽核委員聘任同意暨保密切結書

國立屏北高級中學108年度資通安全稽核計畫

稽核委員聘任同意暨保密切結書

本人_____（以下簡稱甲方）為協助國立屏北高級中學（以下簡稱乙方）執行「資通安全稽核計畫」(以下簡稱本計畫)，接受乙方之邀請，擔任　　年資安稽核團隊之稽核委員，特立書同意事項如下：

- 甲方應遵守國家機密保護法、個人資料保護法、行政院及所屬各機關資訊安全管理要點、行政院及所屬各機關資訊安全管理規範、著作權法及其他相關法令之規定，並對因執行本計畫或因執行本計畫之機會所知悉之機密資訊負有保密義務；且上開各義務不因甲方與乙方或與技服中心間，就本年度擔任稽核委員相關事宜之法律關係解除、終止或完成而失其效力。

- 甲方就因執行本計畫或因執行本計畫之機會，所知悉或接觸之乙方、受稽機關或其他第三人之機密資訊，除因執行本計畫所必須，且事先經乙方書面同意者，或法律另有明文規定外，不得有下列行為：

  甲、 全部或一部重製或留存上開機密資訊；

  乙、 以任何方式向任何第三人揭露上開機密資訊之全部或一部；

  丙、 以任何方式使任何第三人知悉、持有或使用上開機密資訊之全部或一部；

  丁、 以任何方式使自己或任何第三人就上開機密資訊之全部或一部取得任何權利；

  戊、 揭露、公開或使用上開機密資訊之全部或一部。

- 甲方因執行本計畫所製作之報告、文件或其他產出，其智慧財產權及其他權利均歸屬乙方所有。

- 甲方與受稽機關有下列情形之一者，就與該受稽機關之稽核相關事宜，應主動迴避，或事先以書面告知乙方，以確認是否得免予迴避：

  甲、 甲方、甲方之配偶、甲方三親等以內血親或姻親、與甲方有共同生活關係之家屬、或上開人員財產信託之受託人，與受稽機關間，有財產上或非財產上利益之利害關係者；

  乙、 甲方、甲方之配偶、甲方三親等以內血親或姻親、與甲方有共同生活關係之家屬，與受稽機關或其負責人間現有或於過去兩年間曾有僱傭、承攬、委任、代理或其他類似之關係者；

  丙、 甲方或其現任職或於過去兩年內曾任職之機關，於民國105年至本次稽核期間，

曾為受稽機關進行與受稽事項相關之顧問輔導者。

- 前條所稱財產上利益，係指動產、不動產、現金、有價證券、債權、其他財產上權利、具有經濟價值或得以金錢交易取得之利益；所稱非財產上利益，係指有利於甲方之配偶、甲方三親等以內血親或姻親、與甲方有共同生活關係之家屬、或上開人員財產信託之受託人於受稽機關或其關聯機關之任用、陞遷、調動及其他人事措施。

- 有其他情形足認甲方有不能公正執行職務之虞，經受稽機關敘明理由，並由乙方作成迴避決定者，甲方應迴避之。

- 甲方有第四條各款情形之一，而未自行迴避，亦未事先以書面告知乙方相關情事，並經乙方書面同意免予迴避者，乙方得終止本契約，甲方應返還已收取之報酬，如乙方，因此認有必要對受稽核機關重為全部或一部稽核，或受有其他不利益時，甲方並應賠償乙方因此所生之一切損失及費用（包括但不限於賠償金、和解金、律師費及訴訟費用等）。

- 甲方如違反第二條或就相關事宜涉及其他不法情事，將移送司法機關處理；如致乙方、受稽機關，遭受任何不利益，或受第三人法律上請求或訴追者，甲方應賠償乙方、受稽機關，因此所生之一切損失及費用（包括但不限於賠償金、和解金、律師費及訴訟費用等）。

- 甲方應公正執行職務，並應避免使人誤認推薦特定廠商、產品或服務；且處理稽核相關事務或出席會議，應親自為之。

此　致

國立屏北高級中學;

受稽機關

立同意書人

姓　　名：　　（簽章）

身份證字號：

中華民國　　年　　月　　日

13. 稽核結果及改善報告

國立屏北高級中學稽核結果及改善報告

稽核範圍	全機關
稽核日期	107 年 ○○ 月 ○○ 日
審查日期	107 年 ○○ 月 ○○ 日

改善措施				
編號	**稽核缺失或待改善稽核項目**	**改善措施**	**改善期程規劃**	**相關證明資料**
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

單位主管：　　資通安全長：

註：陳核層級請機關依需求調整

14. 改善績效追蹤報告

國立屏北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01月29日10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，並確保備份設備及機制運作效果。	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。
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 01 月 29 日	實際完成日期	108 年 01 月 29 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	○○○

註：陳核層級請機關依需求調整