資通安全維護計畫參考附件

目　次

1. 資通安全推動小組成員及分工表

國立中興大學附屬高級中學
資通安全推動小組成員及分工表

編號：○○

製表日期：110 年 03 月 23 日

單位	職級	職掌事項	分機	備註 （代理人）
校長室	校長	統籌資通安全推動	111	秘書
秘書室	秘書	協調各處室資通安全推動	112	教務主任
教務處	教務主任	成績系統、教材系統、自習座位登記系統管理	301	學務主任
學務處	學務主任	學生資料管理	501	總務主任
總務處	總務主任	公文系統管理	201	輔導室主任
輔導室	輔導室主任	輔導資料管理	701	圖書館主任
人事室	人事主任	人事系統管理	121	主計主任
主計室	主計主任	請購系統管理	131	人事主任
圖書館	圖書館主任	借書系統、公播系統管理	601	資訊媒體組長
圖書館	資訊媒體組長	學校首頁、防毒、郵件服務系統管理、資通安全事件通報	631	圖書館主任
二級主管	組長	資安事項實務面工作		同單位組長

資通安全長[1]：校長

2. 資通安全保密同意書

國立中興大學附屬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

國立中興大學附屬高級中學資通安全需求申請單

編號：○○

申請單位	○○處室(組)	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	資訊媒體組	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[2]	○○○

註：陳核層級請機關依需求調整

2 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

國立中興大學附屬高級中學
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	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○○	○○組	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：資訊媒體組長　　單位主管：圖書館主任

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

國立中興大學附屬高級中學
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

國立中興大學附屬高級中學
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

國立中興大學附屬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。

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

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

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
及應變之程序及機制	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。
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。

單位主管：圖書館主任　　資通安全長[3]：校長

註：陳核層級請機關依需求調整

3 特定非公務機關部分，可能是其資安代表，或單位之資安負責人員。

7. 年度資通安全教育訓練計畫

國立中興大學附屬高級中學○○○年度資通安全教育訓練計畫

壹、依據

國立中興大學附屬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[4]	時數
資通安全專責人員		
資訊人員		
一般人員		
主管人員		

4 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

伍、訓練期程（各機關自行定義）

由各機關自行排定教育訓練期程。

陸、訓練方式（各機關自行定義）

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

國立中興大學附屬高級中學
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	主任	○○○	

9. 資通安全維護計畫實施情形

國立中興大學附屬高級中學
資通安全維護計畫實施情形

編號：○○

本機關(單位)之業務因涉及學生權利，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 鈞部（院）提出本（108）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	本校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	本校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	本校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	本校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	本校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	本校由校長為資通安全長，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	本校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	本校依規定設置一名正式人員兼辦資通安全業務。
	4.2 經費之配置	本校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	本校已於今年○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	本校依資通安全責任等級分級辦法，為資通安全責任等級D級機關。

6. 資通安全風險評估	6.1 資通安全風險評估	本校已於今年○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	本校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	本校已依依安全維護計畫辦理。
	7.2 作業及通訊安全管理	本校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	本校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	本校已依規定進行資通安全事件通報。 本校已依規定於今年○、○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	本校接受情資後，已進行分類評估。
	9.2 資通安全情資之因應措施	本校已接受情資之分類，採取對應之因應措施。
10. 資通安全教育訓練	11.1 資通安全教育訓練要求	本校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	本校已於今年○月辦理資通安全教育訓練。
11. 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	12.1 訂定考核機制並進行考核	本本校建立考核機制，並已依規定進行平時及年終考核。
12. 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	本本校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	本校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	本校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：圖書館主任　　資通安全長：校長

註：陳核層級請機關依需求調整