新北市各級學校資通安全維護計畫相關附件

目　次

1. 資通安全管理代表及推動小組成員分工表 1
2. 資通安全保密同意書 3
3. 資通安全需求申請單 4
4. 資訊及資通系統資產清冊 5
5. 風險評估表 8
6. 資訊資產評價標準表 12
7. 資訊資產風險對應表 13
8. 風險發生可能性評估標準表 22
9. 風險處理表 23
10. 管制區域人員進出登記表 28
11. 委外廠商執行人員保密切結書、保密同意書 29
12. 委外廠商查核項目表 31
13. 年度資通安全教育訓練計畫 31
14. 資通安全認知宣導及教育訓練簽到表 33
15. 資通安全維護計畫實施情形 34
16. 審查結果及改善報告 37
17. 改善績效追蹤報告 38

1. 資通安全管理代表及推動小組成員分工表

新北市立中和國中
資通安全管理代表及推動小組成員及分工表

編號：

製表日期：111 年 11 月 08 日

小組成員	姓名	業務事項	分機	備註 （單位）
資通安全長/ 資通安全管理代表	陳春男	1. 資通安全管理政策及目標之核定及督導。 2. 資通安全責任之分配及協調。 3. 資通安全資源分配。 4. 資通安全防護措施之監督。 5. 資通安全事件之檢討及監督。 6. 資通安全相關規章與程序、制度文件核定。 7. 資通安全管理年度工作計畫之核定 8. 資通安全相關工作事項督導及績效管理。 9. 其他資通安全事項之核定。	201	校長
策略規劃組/ 資安聯絡人	吳彩鳳	1. 資通安全政策及目標之研議。 2. 訂定本校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年度工作計畫。	210	教務主任
	黃潤亭		214	資訊組長

		4. 傳達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	吳瑞宜	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。	203	人事主任
	蔡素芬		205	會計主任
	林玉明		220	學務主任
	陳芝仙		230	總務主任
	曾繁揚		240	輔導主任
	彭慧姿		207	補校主任
	王怡瑩		295	幼兒園主任
	連國鉉		222	資訊科技主席

承辦人:　　單位主管：　　機關首長:

教師兼資訊組長黃潤亭　　[illegible]吳彩鳳　　校長陳春男

2. 資通安全保密同意書

中和國中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

中和國中資通安全需求申請單

編號：○○

申請單位		申請日期	
申請項目		項目名稱	
申請數量		需用日期	
申請類別	□新購 □升級	使用設備	
安裝單位		安裝位置	
用途說明			
申請人		單位主管	
資通安全推動小組	□可列入採購排程 □不可採購	說明：	
資通安全推動小組承辦人員		機關首長	

註：陳核層級請學校依需求調整

4. 資訊及資通系統資產清冊

新北市立中和國中資訊及資通系統資產清冊

編號：○○

製表日期：111 年 12 月 06 日

項次	資產名稱	類別	擁有者/職稱	管理者（部門）	使用者（部門）	存放位置	數量	說明	備註
1.	EVO 派送軟體	軟體資產	資訊組	教務處	全校師生	電腦教室	1 套		
2.	個人電腦主機	實體資產	行政教職員	各辦公室	全校師生	教室、辦公室	382 台		
3.	平板電腦	實體資產	行政教職員	各行政辦公室	全校師生	教室、辦公室	370 台		
4.	Apple MDM 伺服器管理系統	軟體資產	資訊組	教務處	全校師生	資訊機房	1 套		
5.	學校網站	軟體資產	資訊組	資訊組	全體教職員	教育局	1 式	局端雲端機房	
6.	連網型備份主機	實體資產	資訊組	資訊組	資訊組	機房	1 台		
7.	EVO Cloud 伺服器	實體資產	資訊組	資訊組	資訊組	電腦教室	1 台		
8.	監視設備	實體資產	各行政辦公室	總務處	總務處	各辦公室、警衛室	15 套	圍牆、走廊、停車場及門口監視器	
9.	資訊機房	實體	資訊組	資訊組	資訊組	自強樓 4	1 式		

項次	資產名稱	類別	擁有者/職稱	管理者（部門）	使用者（部門）	存放位置	數量	說明	備註
		資產				樓			
10.	電腦與語言教室	實體資產	資訊組研發組	資訊組	全校師生	中和樓自強樓	4 式		
11.	多媒體與智慧教室	實體資產	研發組	研發組	全校師生	自強樓	2 式		
12.	行動充電車	實體資產	資訊組	資訊組	全校師生	中和樓自強樓	12 式		
13.	機房 UPS	支援服務資產	資訊組	資訊組	資訊組	機房	7 台		
14.	機房消防設備	支援服務資產	資訊組	資訊組	資訊組	機房	1 組		
15.	機房空調設備	支援服務資產	資訊組	資訊組	資訊組	機房	2 台		
16.	主管人員	人員資產	校長	校長	校長	辦公室	1 式	主任以上	
17.	教職人員	人員資產	校長	校長	校長	辦公室	1 式	主任以下	
18.	資訊組長	人員資產	教務主任	教務主任	教務主任	辦公室	1 人		
19.	圖書志工	人員資產	資管組	資管組	教務處	圖書室	1 式	接觸學生資料	
20.	教務處教學資料	資訊資產	教學組	教務處	全校教師	NAS	1 式		
21.	教務處專案計畫、公文	資料資產	教務主任	教務處	教務處	教務處	1 式		

項次	資產名稱	類別	擁有者/職稱	管理者（部門）	使用者（部門）	存放位置	數量	說明	備註
22.	學生註冊資料	資料資產	資管組長	資管組	資管組	教務處	1式		
23.	學務處學生健康系統	軟體資產	校護	學務處	校護	健康中心	1式	學生個資資料	
24.	學務處專案計畫、公文、校安通報、性平案與霸凌案件	資料資產	學務主任	學務處	學務處	學務處	1式		
25.	總務處專案計畫、公文、財管資料、地籍資料、出納憑證	資料資產	總務主任	總務處	總務處	總務處	1式		
26.	輔導室專案計畫、公文、個案輔導記錄	資料資產	輔導主任	輔導室	輔導室	輔導室	1式		
27.	人室事履歷資料	資料資產	人事主任	人事室	人事室	人事室	1式	教職員工人事履歷	
28.	幼兒園幼兒個資、教師獎懲文件	資料資產	幼兒園主任	幼兒園	幼兒園	幼兒園	1式		
29.	學生家庭基本資料	資料資產	各老師	各老師	各老師	各老師	1式		

承辦人：

教師兼資訊組長黃潤亭

單位主管：

[illegible]

機關首長:

校長陳春男

5. 風險評估表

中和國中風險評估表

編號：○○

製表日期：111 年 12 月 06 日

項次	資產名稱	資產大類	資產小類	機密性(C)	完整性(I)	可用性(A)	資訊資產價值(T)(C,I,A 取最大值)	潛在風險事件	風險發生可能性(V)	風險值資訊資產價值*(T*V)
1.	EVO 派送軟體	軟體資產	套裝軟體	1	1	3	3	1.2.2	2	6
2.	個人電腦主機	實體資產	個人電腦	1	1	2	2	2.3.3	2	4
3.	平板電腦及行動裝置	實體資產	可攜式設備	1	1	1	1	2.4.3	2	2
4.	Apple MDM 伺服器管理系統	軟體資產	套裝軟體	1	2	2	2	1.2.1	2	4
5.	學校網站	軟體資產	套裝軟體	1	1	1	1	1.2.2	1	1
6.	連網型備份主機	實體資產	電腦主機	2	1	2	2	2.1.3	1	2
7.	EVO Cloud 伺服器	實體資產	伺服器	1	2	2	2	2.1.6	2	4
8.	連網監視設備	實體資產	週邊設備	2	2	2	2	2.6.6	2	4
9.	資訊機房	實體資產	機房及電	2	1	3	3	2.7.1	1	6

項次	資產名稱	資產大類	資產小類	機密性(C)	完整性(I)	可用性(A)	資訊資產價值(T)(C,I,A取最大值)	潛在風險事件	風險發生可能性(V)	風險值資訊資產價值*(T*V)
			腦教室							
10.	電腦與語言教室	實體資產	機房及電腦教室	1	1	2	2	2.7.1	1	2
11.	多媒體與智慧教室	實體資產	機房及電腦教室	1	2	2	2	2.7.2	1	2
12.	行動充電車	支援服務資產	電力	1	1	2	2	6.1.4	1	2
13.	機房 UPS	支援服務資產	電力	1	1	2	2	6.1.2	1	2
14.	機房及電腦教室消防設備	支援服務資產	環控消防	1	1	3	3	6.2.1	1	3
15.	機房空調設備	支援服務資產	環控消防	1	1	2	3	6.2.2	1	3
16.	主管人員	人員資產	主管人員	1	1	1	1	4.2.1	1	1
17.	教職人員	人員資產	一般人員	1	1	1	1	4.3.1	2	2

項次	資產名稱	資產大類	資產小類	機密性(C)	完整性(I)	可用性(A)	資訊資產價值(T)(C,I,A 取最大值)	潛在風險事件	風險發生可能性(V)	風險值 資訊資產價值*(T*V)
18.	資訊組長	人員資產	資訊人員	2	2	1	2	4.1.2	1	2
19.	圖書志工	人員資產	外部人員	2	1	2	2	4.4.1	2	4
20.	教務處 教學資料	資訊資產	電子資料	1	1	1	1	5.1.2	1	1
21.	教務處 專案計畫、公文	資料資產	紙本文件	2	1	1	2	3.1.2	1	2
22.	學生註冊資料	資料資產	紙本文件	3	1	1	3	3.1.4	2	6
23.	學務處 學生健康系統	軟體資產	套裝軟體	2	1	1	2	1.2.2	2	2
24.	學務處 專案計畫、公文、校安通報、性平案與霸凌案件	資料資產	紙本文件	2	1	1	2	3.1.2	1	2
25.	總務處 專案計畫、公文、財管資料、地籍資料、出納憑證	資料資產	紙本文件	2	1	1	2	3.1.2	1	2

項次	資產名稱	資產大類	資產小類	機密性（C）	完整性（I）	可用性（A）	資訊資產價值(T)(C, I, A 取最大值)	潛在風險事件	風險發生可能性（V）	風險值 資訊資產價值*(T*V)
26.	輔導室專案計畫、公文、個案輔導記錄	資料資產	紙本文件	2	1	1	2	3.1.2	1	2
27.	人室事履歷資料	資料資產	紙本文件	3	1	1	3	3.1.4	1	3
28.	幼兒園幼兒個資、教師獎懲文件	資料資產	紙本文件	3	1	1	3	3.1.4	1	3
29.	學生家庭基本資料	資料資產	紙本文件	3	2	2	3	3.1.4	1	3

註：

1. 本表可與資訊及資通系統資產清冊合併使用。
2. 陳核層級請學校依需求調整

承辦人員：　　單位主管：　　機關首長：

教師兼資訊組長 黃潤亭　　教師兼 吳彩鳳　　校長 陳春男

6. 資訊資產評價標準表

評分 / 類型	0	1	2	3
機密性(C)	無此特性或可公開	僅供單位內部人員使用	僅供業務相關人員存取	具特殊權限人員方可存取
完整性(I)	無此特性或不影響單位運作	將造成本校部份業務運作效率降低	將造成本校部份業務運作停頓	將造成本校大部分業務運作停頓
可用性(A)	無此特性或最大可容忍中斷時間 5 天以上	最大可容忍中斷時間 3 天以上，5 天以下	最大可容忍中斷時間 1 天以上，3 天以下	最大可容忍中斷時間 1 天以內

7. 資訊資產風險對應表

中和國中資訊資產風險對應表

資產大類	資產小類	潛在風險事件	管控措施範例說明
1.軟體資產類	1.1 作業系統	1.1.1 未落實作業系統更新/漏洞修補，致使遭受惡意攻擊、資料外洩或其他侵害。	-WSUS 機制失效 -定期檢查漏洞更新狀態 -資訊單位定期彙整提供發佈更新資訊，供業務單位進行比對
1.軟體資產類	1.1 作業系統	1.1.2 未購買妥適的作業系統授權/使用授權超過購買數，致使遭受廠商求償或抗議。	-作業系統授權清單
1.軟體資產類	1.1 作業系統	1.1.3 未汰換原廠公告停止技術支援之作業系統，進而無法修補漏洞，致使遭受惡意攻擊、資料外洩或其他侵害。	
1.軟體資產類	1.1 作業系統	1.1.4 未加入組織之網域，進而無法套用 GCB 或群組原則政策，致使無法有效管控。	-套用 GCB 設定，或設定適當權組原則
1.軟體資產類	1.1 作業系統	1.1.5 個人電腦或伺服器等資訊設備，未安裝適當之防毒軟體或安全防護軟體，於網路連線時遭電腦病毒入侵或被植入惡意程式，致使資料外洩或遭受其他侵害。	
1.軟體資產類	1.1 作業系統	1.1.6 作業系統最高管理權限管制不當，有共用或浮濫設定的情形。	
1.軟體資產類	1.2 套裝軟體	1.2.1 未購買妥適的套裝軟體授權或使用超過購買授權數量，致使可能違反智慧財產權，遭受廠商求償。	-軟體管制清單 -軟體授權資料 -資產管理工具

資產大類	資產小類	潛在風險事件	管控措施範例說明
1.軟體資產類	1.2 套裝軟體	1.2.2 未定期進行套裝軟體更新(含防毒軟體)/漏洞修補，致使遭受惡意攻擊、資料外洩或其他侵害。	-軟體原廠發佈更新及安裝紀錄 -資訊單位定期彙整提供發佈更新資訊，供業務單位進行比對 -定期檢查原廠公告漏洞修補狀態
2.實體資產類	2.1 伺服器	2.1.1 未安裝於機櫃中或實體管制隔離區(如：機房)，可能因人員誤觸或未經授權人員有機會碰觸，而造成設備損壞、資料外洩或服務中斷。	-機房環境管控
2.實體資產類	2.1 伺服器	2.1.2 伺服器擺放位置，未考量安全環境(如：溫度、濕度、電力、監控等)，可能因安全環境背景，造成伺服器損壞或服務中斷。	-機房環境管控
2.實體資產類	2.1 伺服器	2.1.3 伺服器超過廠商保固期限，未定期編列經費維護或汰換，造成設備可能因零件損壞時無料可維修，致使服務中斷。	-超過保固期限
2.實體資產類	2.1 伺服器	2.1.4 伺服器於報廢前未妥善清除資料(備註)，致使資料外洩或遭受其他侵害。	-相關設定與儲存媒體之資料必須清除 -如專業資料清除軟體或實體破壞
2.實體資產類	2.1 伺服器	2.1.5 重要伺服器無適當之備援措施。	-設備備援措施
2.實體資產類	2.1 伺服器	2.1.6 設備安裝或變更無適當管控措施。	-安裝或變更管制措施
2.實體資產類	2.1 伺服器	2.1.7 設備未定期維護或缺乏備援設備，致使設備故障時未能及時修復影響業務。	-定期維護

資產大類	資產小類	潛在風險事件	管控措施範例說明
2.實體資產類	2.2 網路設備	2.2.1 骨幹網路設備未安裝於機櫃中或實體管制隔離區(如：機房)，造成因人員誤觸或未經授權人員有機會接觸設備，而致使設備損壞、資料外洩或服務中斷。	
2.實體資產類	2.2 網路設備	2.2.2 網路設備擺放位置，未考量安全環境(如：溫度、濕度、電力、監控等)，造成因安全環境背景，致使伺服器損壞或服務中斷。	
2.實體資產類	2.2 網路設備	2.2.3 網路設備超過廠商保固期限，未定期編列經費維護或汰換，造成設備可能因零件損壞時無料可維修，致使服務中斷。	
2.實體資產類	2.2 網路設備	2.2.4 設備於報廢前未妥善清除資料，致使資料外洩或遭受其他侵害。	-相關設定與儲存媒體之資料必須清除 -如專業資料清除軟體或實體破壞
2.實體資產類	2.2 網路設備	2.2.5 核心網路設備架構上具有單點失效之問題。	
2.實體資產類	2.2 網路設備	2.2.6 網路纜線接合不良或未做適當防護措施。	
2.實體資產類	2.3 個人電腦	2.3.1 個人電腦超過廠商保固期限，未定期編列經費汰換，造成設備因零件損壞時無料可維修，致使服務中斷。	
2.實體資產類	2.3 個人電腦	2.3.2 個人電腦未進行適切的資產管理及管制硬體規格數量，造成零組件遭置換或遺失，致使硬體效能降低，影響作業效率。	
2.實體資產類	2.3 個人電腦	2.3.3 處理機敏性資料之個人電腦未進行適切的隔離或存取控制措施，可能發生資料外洩。	

資產大類	資產小類	潛在風險事件	管控措施範例說明
2.實體資產類	2.3 個人電腦	2.3.4 未管制個人電腦內建式燒錄機或 USB 連接埠，透過可攜式媒體將資料複製攜出，致使資料於未授權情況下，造成資料外洩、遺失或遭受其他侵害。	-如全面控管，禁止使用 -或設定 USB 僅能讀取資料，禁止寫出 -或特別申請 USB 開放使用，並保存讀取/寫出紀錄 -或僅能使用經組織登錄配發之可攜式媒體(並使用加密功能)
2.實體資產類	2.3 個人電腦	2.3.5 個人電腦於報廢前未妥善清除資料(備註)，致使資料外洩或遭受其他侵害。	-相關設定與儲存媒體之資料必須清除 -如專業資料清除軟體或實體破壞
2.實體資產類	2.4 可攜式設備	2.4.1 存放設備之實體門禁未進行出入管制或長時間不使用時未將設備妥善收存，造成同仁、外部訪客或廠商可能無意/故意將設備攜出，致使設備遺失、資料外洩或遭受其他侵害。	
2.實體資產類	2.4 可攜式設備	2.4.2 設備遺失未即時通報，造成組織未能即時處置，致使資料外洩或遭受其他侵害。	
2.實體資產類	2.4 可攜式設備	2.4.3 未管制筆記型電腦內建式燒錄機或 USB 連接埠，透過可攜式媒體將資料複製攜出，致使資料於未授權情況下，造成資料外洩、遺失或遭受其他侵害。	-如全面控管，禁止使用 -或設定 USB 僅能讀取資料，禁止寫出 -或特別申請 USB 開放使用，並保存讀取/寫出紀錄 -或僅能使用經組織登錄配發之可攜式媒體(並使用加密功能)

資產大類	資產小類	潛在風險事件	管控措施範例說明
2.實體資產類	2.4 可攜式設備	2.4.4 可攜式設備於報廢前未妥善清除資料(備註)，致使資料外洩或遭受其他侵害。	-相關設定與儲存媒體之資料必須清除 -如專業資料清除軟體或實體破壞
2.實體資產類	2.4 可攜式設備	2.4.5 筆記型電腦、平板電腦或智慧型手機等可攜式設備，未安裝適當之防毒軟體或安全防護軟體，於網路連線時遭電腦病毒入侵或被植入惡意程式，致使資料外洩或遭受其他侵害。	
2.實體資產類	2.5 可攜式媒體	2.5.1 可攜式媒體未妥善保管，造成同仁、外部訪客或廠商無意/故意將可攜式媒體攜出，致使媒體遺失、資料外洩或遭受其他侵害。	-如可攜式媒體經申請或借用後，應妥為收藏或上鎖存放 -或機敏資訊儲存於可攜式媒體，應予以加密
2.實體資產類	2.5 可攜式媒體	2.5.2 可攜式媒體攜出組織場所，未妥善保管，致使資料外洩或遭受其他侵害。	-攜出組織場所以外，須將可攜式媒體放置於放置於包裝袋中
2.實體資產類	2.5 可攜式媒體	2.5.3 可攜式媒體於報廢前未妥善清除資料，致使資料外洩或遭受其他侵害。	-如專業資料清除軟體或實體破壞 -或將磁碟/磁帶/磁片予以消磁
2.實體資產類	2.6 週邊設備	2.6.1 列(影)印、傳真機密文件，未即時將紙本文件取走，留置於設備上，造致使資料外洩或遭受其他侵害。	
2.實體資產類	2.6 週邊設備	2.6.2 設備未定期維護或缺乏備品，致使設備故障時未能及時修復影響作業效率。	
2.實體資產類	2.6 週邊設備	2.6.3 設備於報廢前未妥善清除資料，致使資料外洩或遭受其他侵害。	-相關設定與儲存媒體之資料必須清除 -如專業資料清除軟體或實體破壞

資產大類	資產小類	潛在風險事件	管控措施範例說明
2.實體資產類	2.6 週邊設備	2.6.4 保存紙本文件資料或可攜式媒體之文件櫃或硬體設備，應上鎖而未上鎖或上鎖功能損壞，致使資料外洩或遭受其他侵害。	
2.實體資產類	2.6 週邊設備	2.6.5 設備放置於外部網路、權限未適當管控或未進行適當防護，可能遭駭客入侵，做為進入內部網路的跳板。	
2.實體資產類	2.6 週邊設備	2.6.6 設備未定期或自動校時，導致紀錄時間，無法作為證據。	
2. 實體資產類	2.7 機房及電腦教室	2.7.1 資訊機房或電腦教室未設置控管措施，當非授權人員蓄意破壞、偷竊或滲透，致使資訊設備遭毀損、未經授權攜出或資料外洩。	-設置門禁及門口監視器 -設備進出須有放行條
2. 實體資產類	2.7 機房及電腦教室	2.7.2 資訊機房或電腦教室未考量監控措施，致使發生非預期事件或災害時，難以及時處理且事後難以追溯發生原因或提供證據。	-設置機房或電腦教室內設置監視器
2. 實體資產類	2.7 機房及電腦教室	2.7.3 資訊機房未考量適當之防護設施，發生天災或其它環境威脅時無法進入，致使影響正常營運。	-墊高出入口或防水閘門 -防焰材質建築材料
3.資料資產類	3.1 紙本文件	3.1.1 資訊系統相關技術說明、設定或規劃文件，未有適當控管，致使資料遺失、毀損、外洩或遭受其它侵害。	-如文件櫃上鎖存放
3.資料資產類	3.1 紙本文件	3.1.2 業務資料或其它包含機敏資訊之文件，未依安全等級控管，致使資料遺失、毀損、外洩或遭受其它侵害。	-依資訊資產安全等級限閱或敏感等級進行管理
3.資料資產類	3.1 紙本文件	3.1.3 業務資料或其它包含一般資訊之文件，違反組織作業程序或法令法規之要求，致使資料遭不當使用後，影響法律規章遵循或損害組織信譽。	-依資訊資產安全等級一般或公開等級進行管理

資產大類	資產小類	潛在風險事件	管控措施範例說明
3.資料資產類	3.1 紙本文件	3.1.4 包含個人資料之文件，未有適當控管，致使資料遺失、毀損、外洩或遭受其它侵害。	-依個人資料檔案機密等級進行管理
3.資料資產類	3.1 紙本文件	3.1.5 逾保存期限之紙本文件、表單或紀錄，未能適度予以銷毀，造成保存之文件與資料過多，致使發生遺失或外洩情況時，增加組織遭損害求償之風險或損害組織信譽。	-依文件與紀錄管理程序書進行管理
4.人員資產類	4.1 資訊人員	4.1.1 資訊人員未訂定或落實代理人制度，致使組織遇緊急資安事件時無法即時處置。	-資安事件如：網路斷線、系統無法正常使用等
4.人員資產類	4.1 資訊人員	4.1.2 資訊人員未進行適當職務區隔，造成特定人員權限過大，增加組織之營運風險。	
4.人員資產類	4.1 資訊人員	4.1.3 人員的疏失、操作錯誤或惡意行為，致使作業過程中資料外洩或遭受其他侵害。	
4.人員資產類	4.2 主管人員	4.2.1 缺乏職務代理機制，影響組織行政效率或造成管理弊端。	
4.人員資產類	4.2 主管人員	4.2.2 主管人員遭受脅迫、賄絡或社交工程影響，造成機敏資訊外洩或遭受其它侵害，違反組織作業程序或法令法規之要求，致使資料遭不當使用後，影響法律規章遵循、損害組織利益或信譽。	-主管人員擁有較多機敏資訊權限，若其資料外洩或遭受其它侵害時，影響層面較廣
4.人員資產類	4.3 一般人員	4.3.1 人員未瞭解組織資訊安全政策、內部制度規範及應負之資安責任，造成人員資安認知不足，致使作業過程中資料外洩或遭受其他侵害。	
4.人員資產類	4.3 一般人員	4.3.2 人員的疏失、操作錯誤或惡意行為，致使作業過程中資料外洩或遭受其他侵害。	

資產大類	資產小類	潛在風險事件	管控措施範例說明
4.人員資產類	4.3 一般人員	4.3.3 缺乏職務區隔機制，造成承辦人員被賦予之權限過大或不適當，致使產生管理弊端。	-如審查者與設定者需進行適當區隔 -如會計與出納需明確區隔
4.人員資產類	4.3 一般人員	4.3.4 缺乏職務代理機制，造成發生突發狀況時無法及時反應，致使營運中斷或發生資安事故。	
4.人員資產類	4.4 外部人員	4.4.1 未告知外部人員本組織之資訊安全政策及資安要求，造成外部人員資安認知不足或作業疏失，致使組織資料外洩或遭受其他侵害。	
4.人員資產類	4.4 外部人員	4.4.2 人員未能配合、疏失、操作錯誤或惡意行為，致使作業過程中資料外洩或遭受其他侵害。	
4.人員資產類	4.4 外部人員	4.4.3 人員接觸組織資料前未簽訂保密切結或協議，致使人員將組織資料攜出或惡意揭露。	
5.資訊資產類	5.1 電子資料	5.1.1 業務資料或其它包含機敏資訊之電子資料，未依安全等級控管，致使資料遺失、毀損、外洩或遭受其它侵害。	-如限閱或敏感等級存取權限控管 -或加密存放 -或機敏資訊儲存於可攜式媒體，應予以加密。
5.資訊資產類	5.1 電子資料	5.1.2 業務資料或其它包含一般資訊之電子資料，違反組織作業程序或法令法規之要求，致使資料遭不當使用後，影響法律規章遵循或損害組織信譽。	-如一般等級資料存取權限控管 -如公開資料覆核
5.資訊資產類	5.1 電子資料	5.1.3 包含個人資料之電子資料，未有適當控管，致使資料遺失、毀損、外洩或遭受其它侵害。	-依個人資料檔案機密等級進行管理

資產大類	資產小類	潛在風險事件	管控措施範例說明
5.資訊資產類	5.1 電子資料	5.1.4 資料庫包含之各項資料，未有適當控管，致使資料不正確、毀損、外洩或遭受其它侵害。	-如透過 DBMS 寫入、修改或查詢等功能權限控管 -或資料庫加密/欄位加密
6.支援服務資產	6.1 電力	6.1.1 機房未設有不斷電系統或備援發電機，停電時造成系統主機無法得到足夠供電，致使業務無法持續運作或主機無法正常關機。	
6.支援服務資產	6.1 電力	6.1.2 不斷電系統未計算或定期評估可承載容量及耐用年限，停電時造成設備無法得到足夠供電，致使業務無法持續運作或伺服器無法正常關機。	
6.支援服務資產	6.1 電力	6.1.3 機櫃或延長線未設有電流負載偵測功能，致使負載過高時造成跳電進而影響營運作業。	
6.支援服務資產	6.1 電力	6.1.4 行動充電車未設有電流負載偵測功能，致使負載過高時造成跳電進而影響運作。	
6.支援服務資產	6.2 環控消防	6.2.1 設備未定期維護造成失效進而影響營運作業。	
6.支援服務資產	6.2 環控消防	6.2.2 未汰換老舊設備造成失效，進而影響營運作業。	

8. 風險發生可能性評估標準表

風險發生可能性	數值
高	3
中	2
低	1

9. 風險處理表

新北市中和國中風險處理表

編號：○○

製表日期：111 年 12 月 06 日

項次	資產名稱	資產大類	擁有者/職稱	資訊資產價值(T)(C,I,A 取最大值)	潛在風險事件	處理前風險發生可能性(V)	處理前風險值(T*V)	新增控制措施	處理後風險發生可能性(V)	處理後風險值(T*V)
1.	EVO 派送軟體	實體資產	資訊組	3	1.2.2	2	6	定期安裝軟體原廠發佈之更新及安裝	2	6
2.	個人電腦主機	實體資產	全體教職員	2	2.3.3	2	4	定期安裝軟體原廠發佈之更新及安裝	2	4
3.	平板電腦及行動裝置	實體資產	全體教職員	1	2.4.3	2	2	定期安裝軟體原廠發佈之更新及安裝	2	2
4.	Apple MDM 伺服器管理系統	軟體資產	資訊組	2	1.2.1	2	4	將系統移到 Jamf MDM	1	2
5.	學校網站	軟體資產	資訊組	1	1.2.2	1	1	定期安裝軟體原廠發佈之更新及安裝	1	1
6.	連網型備份	實體	資訊	2	2.1.3	1	2	定期安裝	1	2

項次	資產名稱	資產大類	擁有者/職稱	資訊資產價值(T)(C,I,A取最大值)	潛在風險事件	處理前風險發生可能性(V)	處理前風險值(T*V)	新增控制措施	處理後風險發生可能性(V)	處理後風險值(T*V)
	主機	資產	組					軟體原廠發佈之更新及安裝		
7.	EVO Cloud 伺服器	實體資產	資訊組	1	2.1.6	2	2	定期安裝軟體原廠發佈之更新及安裝	2	2
8.	連網監視設備	實體資產	總務處	2	2.6.6	2	4	定期安裝軟體原廠發佈之更新及安裝	2	4
9.	資訊機房	實體資產	資訊組	3	2.7.1	1	3	定期安裝韌體原廠發佈之更新及安裝	1	3
10.	電腦與語言教室	實體資產	資訊/研發組	2	2.7.1	1	2	定期安裝軟體原廠發佈之更新及安裝	1	2
11.	多媒體與智慧教室	實體資產	研發組	2	2.7.2	1	2	定期安裝軟體原廠發佈之更新及安裝	1	2
12.	行動充電車	支援服務資產	資訊組	2	6.1.4	1	2	定期安裝軟體原廠發佈之更	1	2

項次	資產名稱	資產大類	擁有者/職稱	資訊資產價值(T)(C,I,A取最大值)	潛在風險事件	處理前風險發生可能性(V)	處理前風險值(T*V)	新增控制措施	處理後風險發生可能性(V)	處理後風險值(T*V)
								新及安裝		
13.	機房 UPS	支援服務資產	資訊組	1	6.1.2	1	1	定期安裝軟體原廠發佈之更新及安裝	1	1
14.	機房及電腦教室消防設備	支援服務資產	資訊組	1	6.2.1	1	1	定期安裝軟體原廠發佈之更新及安裝	1	1
15.	機房及電腦教室空調設備	支援服務資產	資訊組	1	6.2.2	1	1	定期安裝軟體原廠發佈之更新及安裝	1	1
16.	主管人員	人員資產	校長	1	4.2.1	1	1	依個人資料檔案機密等級進行管理	1	1
17.	教職人員	人員資產	校長	1	4.3.1	2	2	依個人資料檔案機密等級進行管理	2	2
18.	資訊組長	人員資產	教務主任	1	4.1.2	2	2	依個人資料檔案機密等級進行管理	2	2

項次	資產名稱	資產大類	擁有者/職稱	資訊資產價值(T)(C,I,A取最大值)	潛在風險事件	處理前風險發生可能性(V)	處理前風險值(T*V)	新增控制措施	處理後風險發生可能性(V)	處理後風險值(T*V)
19.	圖書志工	人員資產	教務主任	2	4.4.1	1	2	依個人資料檔案機密等級進行管理	1	2
20.	教務處 教學資料	資訊資產	教學組	1	5.1.2	1	1	依個人資料檔案機密等級進行管理	1	1
21.	教務處 專案計畫、公文	資料資產	教務主任	2	3.1.2	1	2	依個人資料檔案機密等級進行管理	1	2
22.	學生註冊 資料	資料資產	註冊組長	2	3.1.4	2	4	依個人資料檔案機密等級進行管理	2	4
23.	學務處 學生健康資料	紙本文件	校護	2	3.1.4	1	2	依個人資料檔案機密等級進行管理	1	2
24.	學務處 專案計畫、公文、校安通報、性平案與霸凌案件	資料資產	學務主任	2	3.1.2	1	2	依個人資料檔案機密等級進行管理	1	2
25.	總務處	資料	總務	2	3.1.2	1	2	依個人資料檔案機	1	2

項次	資產名稱	資產大類	擁有者/職稱	資訊資產價值(T)(C, I, A取最大值)	潛在風險事件	處理前風險發生可能性(V)	處理前風險值(T*V)	新增控制措施	處理後風險發生可能性(V)	處理後風險值(T*V)
	專案計畫、公文、財管資料、地籍資料、出納憑證	資產	主任					密等級進行管理		
26.	輔導室 專案計畫、公文、個案輔導記錄	資料資產	輔導主任	3	3.1.2	1	3	依個人資料檔案機密等級進行管理	1	3
27.	人室事 履歷資料	資料資產	人事主任	3	3.1.4	1	3	依個人資料檔案機密等級進行管理	1	3
28.	幼兒園 幼兒個資、教師獎懲文件	資料資產	園長	3	3.1.4	1	3	依個人資料檔案機密等級進行管理	1	3
29.	學生家庭基本資料	資料資產	各老師	2	3.1.4	1	2	依個人資料檔案機密等級進行管理	1	2

承辦人員：　　單位主管：　　機關首長：

教師兼資訊組長黃潤亭　　校長陳春男

10. 管制區域人員進出登記表

中和國中管制區域人員進出登記表

編號：

製表日期：　　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
範例	王○○	○○室	陳○○	107.12.2	8：00	9：00	教學軟體安裝	普	個人筆電	外接磁碟

註：表格不限紙本記錄，可由電子表單列印

承辦人：　　單位主管：

11. 委外廠商執行人員保密切結書、保密同意書

新北市立中和國民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）委派至新北市立中和國民中學（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

新北市立中和國民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）取得新北市立中和國民中學（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

12. 委外廠商查核項目表

不須執行委外廠商查核。

13. 年度資通安全教育訓練計畫

中和國中資通安全教育訓練計畫

壹、依據

依據資通安全管理法及「資通安全責任等級分級辦理」規定，本市各級學校屬 D 級需完成每人每年接受 3 小時以上之資通安全通識教育訓練，教育局提供取得資通安全通識教育訓練課程之管道。

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，對象以學校支領固定月薪之教職員為主。

肆、訓練內容

資訊安全基礎認知、校園常見資安事件、資通安全文件管理、資通安全導入實作。

伍、訓練期程

由各教職員自行選定。

陸、訓練方式

(一) 本校辦理之資通安全實體課程研習

(二)教育部、教育局或本校辦理之資通安全研習

(三)新北市政府教育局數位學習影音網，網址 https://estudy.ntpc.edu.tw/，課程總攬-資訊安全課程。

(四)教育部教師 e 學院，網址 https://ups.moe.edu.tw/mooc/index.php

(五)e 等公務園學習平臺，網址 https://elearn.hrd.gov.tw/mooc/index.php。

14. 資通安全認知宣導及教育訓練簽到表

中和國中資通安全認知宣導及教育訓練

簽到表

編號：○○○

課程名稱：

時　　間：

地　　點：

15. 資通安全維護計畫實施情形

中和國中資通安全維護計畫實施情形

編號：○○

本校經主管機關核定後本校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，向上級機關提出本 111 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，請學校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. 資通業務及其重要性	1.1 資通業務及重要性盤點	本校資通業務及重要性詳參資通安全維護計畫（詳附件）。
2. 資通安全政策及目標	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，並經校長核定(詳附件)。
	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. 設置資通安全推動代表	3.1 設定資通安全管理代表	本校訂定校長為資通安全管理代表
	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. 人力及經費之配置	4.1 人員配置	資通安全責任等級 D 級學校無需設置資通安全專責人員，惟本校仍設置 1 人，由資訊組長兼任。
	4.2 經費之配置	本校今年未配置資安專用經費。
5. 資訊及資通系統	5.1 資訊及資通系統之盤點	本校已於今年 12 月盤點資訊、資通

之盤點及資通系統、相關資產之標示		系統，建立資產目錄。
	5.2 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 12 月完成資訊、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 資訊及資通系統之保管	本校已依依安全維護計畫辦理，詳附件資料。
	7.2 存取控制與加密機制管理	本校已依資通安全維護計畫辦理。
	7.3 作業及通訊安全管理	本校已依資通安全維護計畫辦理。
	7.4 資通安全防護設備	本校已依資通安全維護計畫辦理。
8. 資通安全事件通報、應變及演練	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。 本校已依規定完成通報應變演練。
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	本校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	本校已依規定監督受託者資通安全維護情形。
11. 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 2 月、8 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	

員辦理業務涉及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檢核機制	本校已依規定辦理內部自我檢核。
	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		

註：陳核層級請學校依需求調整

承辦人: 單位主管： 機關首長：

16. 審查結果及改善報告

中和國中審查結果及改善報告

範圍	全機關
日期	○○○年○○月○○日
審查日期	○○○年○○月○○日

項目				
編號	**建議或待改善項目**	**改善措施**	**改善期程規劃**	**相關佐證資料**
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

17. 改善績效追蹤報告

中和國中改善績效追蹤報告

編號：○○

製表日期：○○○年○○月○○日

審查發現			
審查日期	○○○年○○月○○日○○時	受審查單位	○○○
審查區域	■		
建議或待改善項目與內容			
影響範圍評估			
發生原因分析			

改善措施成效追蹤			
改善措施		預計成效	執行情況
管理面			
技術面			
人力面			
資源面			
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		經費執行情形	

預定完成日期	○○○年○○月○○日	實際完成日期	○○○年○○月○○日
完成進度或情形說明			
改善成效考核			
後續成效追蹤			

承辦人: 單位主管：