文件版本：NTPC11408

新北市各級學校資通安全維護計畫相關附件

目　次

1. 資通安全維護計畫執行事項表

資通安全維護計畫執行事項表

基於資通安全維護計畫提醒資訊組長須完成相關作業事項。

應完成作業項目	資安維護計畫章節編號
1. 確認資通安全推動小組成員	壹拾捌、資通安全管理代表及推動小組成員分工表
2. 校務行政帳號與權限管理	玖、資通安全防護及控制措施 二、存取控制與加密機制管理 (三) 校務行政系統帳號與權限管理
3. 資安目標量測	肆、資通安全政策及目標 二、資通安全目標 (一)量化型目標
	壹拾伍、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、資通安全維護計畫之持續精進及績效管理 (二)管理審查議題應包含下列討論事項： 3.資通安全績效之回饋，包括： (1) 資通安全政策及目標之實施情形。
4. 資產盤點與風險評鑑	捌、資通安全風險評估
	壹拾伍、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、資通安全維護計畫之持續精進及績效管理 (二)管理審查議題應包含下列討論事項： 3.資通安全績效之回饋，包括： (4)風險評鑑結果及風險處理計畫執行進度。
5. 委外資安要求	壹拾貳、資通服務委外辦理之管理
6. 資安情資處理	壹拾壹、接獲資通安全情資之評估及因應
7. 召開管理審查會議	壹拾伍、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、資通安全維護計畫之持續精進及績效管理

2. 資通安全管理審查會議紀錄

○○○○（學校名稱）資通安全管理審查會議紀錄

註：此為學年度需做成之會議紀錄，請保留八項會議討論事項與其子項，並逐項留下校內討論紀錄。

<table>
<tr><td>時間</td><td>○○○年○○月○○日(星期○)上/下午○○時</td></tr>
<tr><td>地點</td><td>○○○</td></tr>
<tr><td>主席</td><td>○○○</td></tr>
<tr><td>紀錄</td><td>○○○</td></tr>
<tr><td>出席人員</td><td>參見簽到表(檢附會議簽到表)</td></tr>
<tr><td>會議
討論事項</td><td>(1) 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。

本校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 D 級，不允許學校自行架設網站。

在使用 FTP 相關服務時，應關閉 FTP 匿名登入功能，並建立個人用傳輸檔案的帳號密碼,如果印表機／事務機及伺服器／個人電腦暴露在 Internet 上,又未限制連線 IP 的話，代表任何人都可以透過 FTP 軟體隨意存取設備上的資料,這類型的設備除了有機敏資料外洩之風險外，還有可能被植入惡意程式，造成嚴重的資安漏洞。

(2) 資通安全維護計畫內容之適切性。

無修正。

(3) 資通安全績效之回饋，包括：

A. 資通安全政策及目標之實施情形。

<table><tr><th>指標</th><th>達成情形</th></tr><tr><td>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。</td><td>資通安全事件__件
於時限內完成__件</td></tr></table></td></tr>
</table>

	逾時完成__件
行政電腦防毒軟體100%啟用，並確保作業系統之更新。	行政電腦__部 防毒軟體啟用__部 作業系統已更新到最新__部
每人每年接受 3 小時以上之資通安全通識教育訓練。	落實狀況良好，同仁均達成法定資安研習時數。 (召開會議當下如仍有同仁未完成，於此格紀錄未完成教育訓練人員名單，並註記後續追蹤補繳研習證明期限)

B. 人力及資源之配置之實施情形。

資訊組長一人；資訊業務協行一名。

C. 資通安全防護及控制措施之實施情形。

落實狀況良好。

D. 不符合項目及矯正措施。

無。

(4) 風險評鑑結果。

風險等級高：0 項

風險等級中：8 項

風險等級低：25 項

風險等級高須處理事項：無

(5) 資通安全事件之處理及改善情形。

無資安事件/

資安事件ＯＯ則；簡述處理狀況。

(6) 利害關係人之回饋。

學科老師提出 OOOO 回饋；行政單位提出 OOOO 回饋；

	學生提出 OOOO 回饋；若無，可寫無。 (7) 持續改善之機會。 公用電腦區重灌頻率可由一年一次改為一學期一次;瀏覽器預設已無痕視窗方式開啟，減少帳號忘記登出之問題。（此處可寫一些「還能做得更好」、且也能夠落實的資安做為，若無則寫無。） (8) 其他。

承辦人：　　單位主管：　　資安長：

3. 資訊資產評價標準表

資訊資產評價標準表

註：繳交成果時無須上傳。

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

4. 資訊資產風險對應表

資訊資產風險對應表

註：校內留存備查，繳交成果時無須上傳。

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	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	1.1 作業系統	1.1.2 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	1.1 作業系統	1.1.3 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	1.1 作業系統	1.1.4 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	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
1.軟體資產	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 -定期檢查原廠公告漏洞修補狀態
2.實體資產	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

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	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	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	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	2.1 伺服器	2.1.5 設備安裝或變更無適當登記與管控措施。	-安裝或變更管制措施與記錄
2.實體資產	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	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	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	2.2 網路設備	2.2.4 網路纜線接合不良或未做適當防護措施。	
2.實體資產	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。	

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	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	2.3 個人電腦	2.3.3 個人電腦之個資或具敏感性資料未進行加密儲存或存取控制措施，可能發生資料外洩。	
2.實體資產	2.3 個人電腦	2.3.4 個人電腦於報廢前未妥善清除儲存之資料，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	2.4 可攜式設備	2.4.1 存放設備之實體門禁未管制出入，或長時間不使用時未將設備妥善收存，造成他人、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	2.4 可攜式設備	2.4.2 設備攜出設備遺失未即時通報，致使資料外洩或遭受其他侵害。	
2.實體資產	2.4 可攜式設備	2.4.3 可攜式設備於報廢前未妥善清除資料，致使儲存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	2.4 可攜式設備	2.4.4 筆記型電腦、平板電腦或智慧型手機等可攜式設備，未定期連線執行作業系統更新或病毒碼更新，而導致於網路連線時，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	2.5 可攜式媒體	2.5.1 可攜式媒體未妥善保管，造成他人、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。	-可攜式媒體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

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	2.5 可攜式媒體	2.5.2 可攜式媒體攜出未妥善保管，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包裝袋中，妥善收存
2.實體資產	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。	-如專業資料清除軟體或實體破壞
2.實體資產	2.5 可攜式媒體	2.5.4 可攜式媒體儲存個資或具敏感性資料未加密，致使資料外洩。	
2.實體資產	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，致使資料外洩或遭受其他侵害。	
2.實體資產	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	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
2.實體資產	2.6 週邊設備	2.6.4 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	2.6 週邊設備	2.6.5 設備未定期或自動校時，導致紀錄時間不正確，無法作為數位證據。	
2.實體資產	2.6 週邊設備	2.6.6 多功能事務機掃描檔案使用 ftp 功能，未設定密碼或使用匿名登入。	
2.實體資產	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、未經授權攜出零件或資料外洩。	-設置門禁及門口監視器 -設備進出須有放行條
2.實體資產	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	-設置機房或電腦教室內設置監視器

資產大類	資產小類	潛在風險事件	管控措施範例說明
		時，難以及時處理且事後難以追溯發生原因或提供證據。	
2.實體資產	2.7 機房及電腦教室	2.7.3 資訊機房或電腦教室設置乾粉滅火器，火災發生使用，將導致電腦設備損壞。	-使用新海龍、環保氣體或二氧化碳滅火器
2.實體資產	2.7 機房及電腦教室	2.7.4 報廢不斷電設備或電池未移出機房，有發生自然的風險。	
2.實體資產	2.7 機房及電腦教室	2.7.5 資訊機房內堆置大量紙箱，火災發生時有助燃的風險。	
2.實體資產	2.8 儲存裝置	2.8.1 儲存裝置韌體未更新到最新版本，可能因系統漏洞導致遭入侵，儲存資料遭竊取或破壞。	
2.實體資產	2.8 儲存裝置	2.8.2 儲存裝置未啟動防毒機制，導致遭病毒入侵，儲存資料遭竊取或破壞。	
2.實體資產	2.8 儲存裝置	2.8.3 未建立定期離線備份機制，儲存資料遭加密或破壞，無法進行復原。	
3.資料資產	3.1 紙本文件	3.1.1 公務資料、個資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	3.1 紙本文件	3.1.2 逾保存期限之紙本文件、表單或紀錄，未進行適當銷毀，導致文件資料外洩。	-依文件與紀錄管理程序書進行管理
4.人員資產	4.1 資訊人員	4.1.1 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	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。	

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	4.3 一般人員	4.3.1 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	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。	
4.人員資產	4.4 外部人員	4.4.1 委外廠商工程師或圖書館志工接觸資訊設備或個資前，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	5.1 電子資料	5.1.1 公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 公務資料或其它包含一般資訊之電子資料，違反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 個資之電子資料，儲存或備份未加密或適當控管，致使資料遺失、毀損、外洩或遭受其它侵害。	-備份資料須依個人資料檔案機密等級進行管理
6.支援服務資產	6.1 電力	6.1.1 機房未設有不斷電系統，停電時造成系統主機無法得到足夠供電正常停機，致使影響業務運作、網路設備或伺服器無法正常關機。	
6.支援服務資產	6.1 電力	6.1.2 不斷電系統未定期更換電池或答耐用年限，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 機櫃延長線未設有突波偵測或防雷擊功能，致使發生突波或雷擊造成設備故障。	

資產大類	資產小類	潛在風險事件	管控措施範例說明
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，致使負載過高或電壓過低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 二氧化碳手提滅火器未定期秤重維護。造成氣壓不足而無法有效滅火。	
6.支援服務資產	6.2 環控消防	6.2.2 未監控機房溫溼度，機房溫濕度過高，導致影響資訊設備運作。	設置溫濕度計進行監控

5. 風險發生可能性評估標準表

風險發生可能性評估標準表

註：繳交成果時無須上傳。

風險發生可能性	數值
每學年可能發生 3 次以上	3
每學年可能發生 1 次未達 3 次	2
每學年可能發生 1 次以下	1

6. 資訊及資通系統資產清冊與風險評估表

○○○○（學校名稱）資訊及資通系統資產清冊與風險評估表

註：如欲刪除範例資產，請先確定學校完全無此項資產方可刪除。各項資產廠牌、型號、數量請依學校實際狀況撰寫。

製表日期：○○○年○○月○○日

項次	資產名稱	廠牌	型號	數量	備註	資產大類	資產小類	管理者（部門）	使用者（部門）	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)	風險等級
1.	電腦教室還原主機	群輝	NTPC-EVO Cloud	3 台		2.實體資產	2.1 伺服器	資訊組	資訊組	1	2	2	2	2.1.5	2	4	中
2.	L3 交換器	D-Link	NTPC-DL	1 部	路由交換器	2.實體資產	2.2 網路設備	資訊組	資訊組	1	1	3	3	2.2.2	1	3	低
3.	個人電腦	Acer	NTPC-4670	250 部		2.實體資產	2.3 個人電腦	資訊組	全體教職員	1	1	2	2	2.3.2	2	4	中
4.	筆電	ASUS	NTPC-NB	20 部		2.實體資產	2.4 可攜式設備	資訊組	全體教職員	1	1	1	1	2.4.4	2	2	低
5.	平板	ASUS	NTPC-chromeboo	60 部		2.實體資產	2.4 可攜式設備	資訊組	全體教職員	1	1	1	1	2.4.1	2	2	低

項次	資產名稱	廠牌	型號	數量	備註	資產大類	資產小類	管理者(部門)	使用者(部門)	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)	風險等級
			k														
6.	平板	Apple	NTPC-Ipad	40 部		2.實體資產	2.4 可攜式設備	資訊組	全體教職員	1	1	1	1	2.4.1	2	2	低
7.	平板	Microsoft	NTPC-surface	40 部		2.實體資產	2.4 可攜式設備	資訊組	全體教職員	1	1	1	1	2.4.1	2	2	低
8.	教室觸控顯示器	盛源	NTPC-TV	40 台		2.實體資產	2.6 週邊設備	資訊組	全體教職員	1	1	2	2	2.6.1	1	2	低
9.	印表機	HP	NTPC-printer	8 部		2.實體資產	2.6 週邊設備	資訊組	全體教職員	1	1	2	2	2.6.1	1	2	低
10.	多功能事務機	FUJIFILM	NTPC-printer2	4 部	具有列印、掃描、影印功能	2.實體資產	2.6 週邊設備	總務處	全體教職員	1	1	2	2	2.6.6	2	4	中
11.	保全系統主機	SE	NTPC-SE	1 部		2.實體資產	2.6 週邊設備	總務處	總務處	2	2	2	2	2.6.4	2	4	中

項次	資產名稱	廠牌	型號	數量	備註	資產大類	資產小類	管理者(部門)	使用者(部門)	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)	風險等級
12.	監視器主機	MO	NTPC-MO	2台		2.實體資產	2.6週邊設備	總務處	總務處	3	2	2	3	2.6.5	2	6	中
13.	公發可攜式媒體	N/A	N/A	1式		2.實體資產	2.5可攜式媒體	全體教職員	全體教職員	1	1	1	1	2.5.2	2	2	低
14.	資訊機房	N/A	N/A	1間		2.實體資產	2.7機房及電腦教室	資訊組	資訊組	3	1	3	3	2.7.4	2	6	中
15.	電腦教室	N/A	N/A	2間		2.實體資產	2.7機房及電腦教室	資訊組	全體教職員	1	1	2	2	2.7.3	2	4	中
16.	教務處專案計畫、公文	N/A	N/A	1式		3.資料資產	3.1紙本文件	教務處	教務處	2	1	1	2	3.1.1	1	2	低
17.	學生註冊資料	N/A	N/A	1式		3.資料資產	3.1紙本文件	註冊組	註冊組	3	1	1	3	3.1.1	1	3	低

項次	資產名稱	廠牌	型號	數量	備註	資產大類	資產小類	管理者(部門)	使用者(部門)	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)	風險等級
18.	學務處專案計畫、公文、校安通報、性平案與霸凌案件	N/A	N/A	1式		3.資料資產	3.1紙本文件	學務處	學務處	3	1	1	3	3.1.1	1	3	低
19.	學生家庭基本資料	N/A	N/A	1式		3.資料資產	3.1紙本文件	導師	導師	3	2	2	3	3.1.1	1	3	低
20.	總務處專案計畫、公文、財管資料、地籍資料、出納憑證	N/A	N/A	1式		3.資料資產	3.1紙本文件	總務處	總務處	2	1	1	2	3.1.1	1	2	低
21.	輔導室專	N/A	N/A	1式		3.資料	3.1紙本	輔導室	輔導室	3	1	1	3	3.1.1	1	3	低

項次	資產名稱	廠牌	型號	數量	備註	資產大類	資產小類	管理者（部門）	使用者（部門）	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)	風險等級
	案計畫、公文、個案輔導記錄					資產	文件										
22.	人室室履歷資料	N/A	N/A	1式		3.資料資產	3.1紙本文件	人事室	人事室	3	1	1	3	3.1.1	1	3	低
23.	教師獎懲文件	N/A	N/A	1式		3.資料資產	3.1紙本文件	人事室	人事室	3	1	1	3	3.1.1	1	3	低
24.	會計憑證資料	N/A	N/A	1式		3.資料資產	3.1紙本文件	會計室	會計室	3	1	1	3	3.1.1	1	3	低
25.	主管人員	N/A	N/A	1式	主任以上	4.人員資產	4.2主管人員	校長	學校	1	1	1	1	4.2.1	1	1	低
26.	教職人員	N/A	N/A	1式		4.人員資產	4.3一般人員	校長	學校	1	1	1	1	4.3.1	2	2	低
27.	資訊組長	N/A	N/A	1人		4.人員	4.1資訊	教務處	全體教職員	2	2	1	2	4.1.1	1	2	低

項次	資產名稱	廠牌	型號	數量	備註	資產大類	資產小類	管理者（部門）	使用者（部門）	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)	風險等級
						資產	人員										
28.	圖書志工	N/A	N/A	1式	接觸學生資料	4.人員資產	4.4外部人員	教務處	教務處	2	1	2	2	4.4.1	2	4	中
29.	教務處教學資料	N/A	N/A	1式		5.資訊資產	5.1電子資料	教務處	全體教職員	1	1	1	1	5.1.2	1	1	低
30.	機房不斷電系統	飛瑞	NTPC-UPS	4台		6.支援服務資產	6.1電力	資訊組	資訊組	1	1	2	2	6.1.2	1	2	低
31.	行動充電車	N/A	N/A	6台	設置於智慧教室	6.支援服務資產	6.1電力	資訊組	全體教職員	1	1	2	2	6.1.4	1	2	低
32.	機房消防設備	N/A	N/A	1組	手提氣體式滅火器	6.支援服務資產	6.2環控消防	資訊組	資訊組	1	1	3	3	6.2.1	1	3	低
33.	機房空調	N/A	N/A	2台		6.支援	6.2環控	資訊組	資訊組	1	1	2	3	6.2.2	1	3	低

項次	資產名稱	廠牌	型號	數量	備註	資產大類	資產小類	管理者（部門）	使用者（部門）	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)	風險等級
	設備					服務資產	消防										

承辦人：　　單位主管：　　資安長：

附註：

1.風險值 1~3 為風險等級低、風險值 4~6 為風險等級中、風險值 7~9 為風險等級高。

2.風險等級高在管理審查會議討論須處理的事項。

7. 管制區域人員進出登記表

○○○○（學校名稱）管制區域人員進出登記表

編號：○○○(學年度)-第○學期

註：每學期核章一次，校內留存備查，繳交成果時無須上傳。

編號	姓名	單位	陪同人員	日期	進入時間	離開時間	事由	攜帶物品
1	王○○	○○室	陳○○	114/10/2	8：00	9：00	機房設備維護	手機

承辦人：　　單位主管：

8. 資通安全需求申請單

○○○○（學校名稱）資通安全需求申請單

編號：○○○(年)-○○(序號)

註：僅機房設備變更須填寫，簽核後校內留存備查，繳交成果時無須上傳。

承辦人		申請日期	○○○年○○月○○日
申請項目	□軟體 □硬體 □其他	軟硬體名稱	
申請數量		需用日期	○○○年○○月○○日
申請類別	□新購 □變更 □移除	使用設備	□網路設備 □主機 □其他
用途說明			

承辦人：　　單位主管：

9. 資通安全保密同意書

○○○○（學校名稱）資通安全保密同意書

編號：○○○(年)-○○(序號)

註：本表供非學校編制內人員填寫（例如圖書館志工、替代役，若無則免填）；不含委外廠商，委外廠商請填寫委外廠商保密同意書、執行人員保密切結書。簽核後校內留存備查，繳交成果時無須上傳。

立同意書人_____於民國____年____月____日起擔任_____(職務)，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、遵守其他本校資通安全相關之法令及規定。

四、如有危害本校資通安全之行為，願負相關之責任。

立同意書人：_____(簽章)

身份證字號：_____(填寫前六碼)

服務學校：_____

資安長：_____

中　　華　　民　　國　　年　　月　　日

10. 委外廠商保密同意書

○○○○（學校名稱）委外廠商保密同意書

編號：○○○(年)-○○(序號)
註：每次簽約時由廠商代表簽署。校內留存備查即可，繳交成果時無須上傳。

茲緣＿＿＿＿＿＿（廠商名稱，以下稱廠商）承接＿＿＿＿＿＿（名稱）（以下稱機關）＿＿＿＿＿＿（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：

第四條　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。

第五條　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。

第六條　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。

第七條　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。

第八條　本同意書一式貳份，機關及----------（廠商）各執存一份。

廠商名稱及蓋章：

廠商負責人姓名及簽章：

廠商地址：

中　　華　　民　　國　　年　　月　　日

11. 委外廠商執行人員保密切結書

○○○○（學校名稱）委外廠商執行人員保密切結書

編號：○○○(年)-○○(序號)

註：校內留存備查即可，繳交成果時無須上傳。

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(填寫前六碼)	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

12. 訪視結果及學校改善報告

○○○○（學校名稱）訪視結果及學校改善報告

註：本表僅受訪視學校須填寫，收到訪視結果報告後 30 日填寫改善措施與預定完成日期，並核章後掃描寄回本局承辦人。學校以學期為單位進行追蹤，全數完成後核章並掃描寄回本局承辦人。

填表日期	○○○年○○月○○日				
訪視日期	○○○年○○月○○日				
項目					
編號	**建議或待改善項目**	**改善措施**	**預定完成日期**	**實際完成日期**	**相關佐證資料**
1.					
2.					
3.					
4.					
5.					

承辦人：　　單位主管：　　資安長：