國立苑裡高級中學資通安全維護計畫 V4.0附件

附件1：資通安全政策
附件2：資通安全組織
附件3：資通安全組織成員表
附件4：保密切結書
附件5：經費配置表
附件6：資通資產管理
附件7：風險評鑑與管理
附件8：資通資產異動作業
附件9：存取控制管理
附件10：實體安全管理
附件11：通信與作業管理
附件12：系統開發與維護
附件13：備份資料回復測試紀錄
附件14：資通安全事件通報應變程序
附件15：委外廠商資安管理作業自評表
附件16：委外廠商保密同意書
附件17：委外廠商執行人員保密切結書
附件18：委外廠商查核暨自我檢核項目表
附件19：資通安全教育訓練統計表
附件20：內部稽核計畫
附件21：稽核項目紀錄表
附件22：內部稽核報告
附件23：矯正與預防處理單

附件1

國立苑裡高級中學-資通安全政策					
文件編號	NYLSH-ISMS-01-001	機密等級	一般	版次	4.0

1 目的

為確保國立苑裡高級中學（以下簡稱本校）所屬之資通資產的機密性、完整性、可用性及法律遵循性，導入資訊安全管理系統，強化本校資通安全管理，保護資通資產免於遭受內、外部蓄意或意外之威脅，維護資料、系統、設備及網路之安全，提供可靠之資訊服務，訂定本政策。

2 依據

2.1 資通安全管理法及子法

2.2 個人資料保護法及施行細則

2.3 教育體系資通安全暨個人資料管理規範

3 適用範圍

3.1 本政策適用範圍為本校之全體人員、委外服務廠商與訪客等。

3.2 資訊安全管理範疇之資訊安全控制領域分為四大主題：組織安全管理、人員安全管理、實體安全管理、技術安全管理。

4 目標

維護本校資通資產之機密性、完整性與可用性，並保障使用者資料隱私。藉由本校全體同仁共同努力來達成下列定性及定量目標：

4.1 定性目標：

4.1.1 符合政府資通安全相關政策、規定及相關法令要求。

4.1.2 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。

4.2 定量目標：

4.2.1 防範惡意電子郵件進行社交工程演練，訂定社交工程郵件開啟率、社交工程郵件點閱率、社交工程郵件附件開啟率。

4.2.2 定期實施資通安全教育訓練。

4.2.3 針對非核心且對外服務之資通系統，每年辦理一次備

份資料回復測試紀錄（附件13)。

4.3 本校完成指標時，考量下列項目：

4.3.1 所需配置之人員、預算、設備技術與程序表單。

4.3.2 活動或事項負責人員。

4.3.3 活動或事項預計完成時間。

4.3.4 管理目標是否達成之評估方式。

5 責任

5.1 本校依據資通安全組織成立資通安全委員會，統籌資通安全事項推動。

5.2 管理階層應積極參與及支持資通安全管理，並授權資通安全組織透過適當的標準和程序以實施本政策。

5.3 本校全體人員、委外服務廠商與訪客等皆應遵守相關安全管理程序以維護本政策。

5.4 本校全體人員及委外服務廠商均有責任透過適當通報機制，通報資通安全事件或弱點。

5.5 任何危及資通安全之行為，將視情節輕重追究其民事、刑事及行政責任或依據本校之相關規定進行議處。

6 審查

本政策應每年至少審查一次，以反映政府法令、技術及業務等最新發展現況及關注方之關注議題，以確保本校資通安全管理運作。

7 實施

本政策經「資通安全委員會」核定後實施，修訂時亦同。

8 相關文件

8.1 備份資料回復測試紀錄

附件2

國立苑裡高級中學-資通安全組織					
文件編號	NYLSH-ISMS-01-002	機密等級	限閱	版次	4.0

1 目的

確保國立苑裡高級中學（以下簡稱本校）資通安全責任，落實資通安全政策之推行，並符合資通安全管理法及子法：

1.1 為確保本校內部資通安全管理事項之推動，應建立適當管理架構，以審核資通安全政策、分配安全責任，並協調本校各項資通安全措施之實施。

1.2 建立與外部資通安全專家之聯繫管道，以利於安全事件處理及專家意見徵詢。

2 適用範圍

本校承辦之資通安全相關業務作業流程。

3 權責

無。

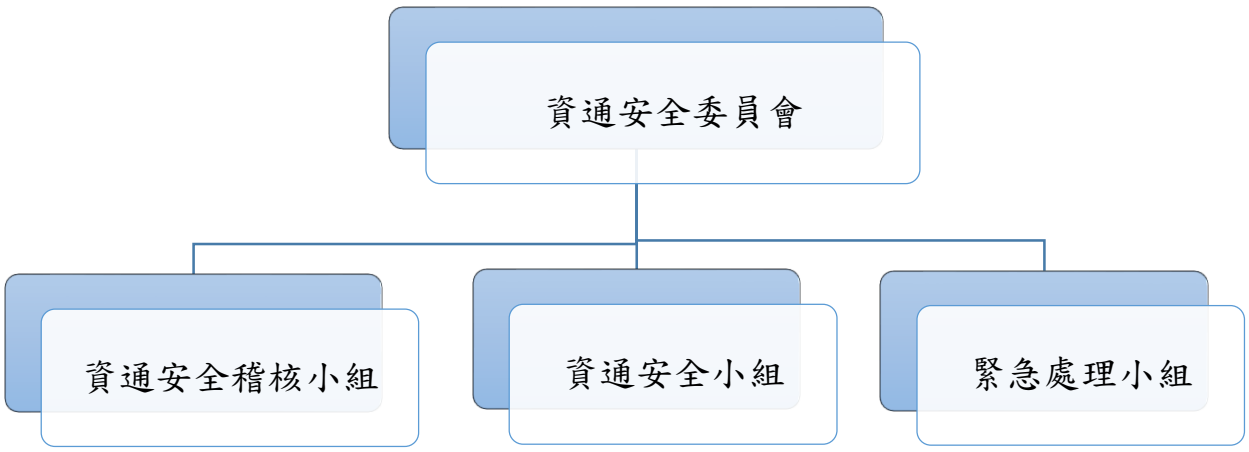
4 名詞定義

無。

5 作業說明

5.1 資通安全組織架構與工作執掌

5.1.1 資通安全組織架構如下圖所示，資通安全組織成員應填寫於「資通安全組織成員表」，人員異動亦即時更新。



5.1.2 資通安全委員會：由本校校長擔任資安長，各單位一級主管、各科主任為委員會委員，負責資通安全管理相關事項之決議。

5.1.2.1 每年定期或視需要召開會議，審查資通安全管理相關事宜。

5.1.2.2 視需要召開跨部門之資源協調會議，負責協調資通安全管理執行所需之相關資源分配。

5.1.3 資安執行秘書：由資安長指派專人擔任。

5.1.3.1 負責協調資通安全小組與緊急處理小組執行資通安全相關作業。

5.1.3.2 負責對資通安全狀況進行預警、監控，並對資通安全狀況與事件進行處置。

5.1.3.3 對於資通安全管理之改善提出建議，以及協助執行資通安全之自我檢核。

5.1.3.4 對於存取控制管理定期進行事件紀錄檢核，以及管理程序檢核。

5.1.4 資通安全小組：由資安長指派人員組成，負責規劃及執行各項資通安全作業。

5.1.4.1 制定資通安全管理相關規範。

5.1.4.2 推動資通安全相關活動。

5.1.4.3 辦理資通安全相關教育訓練。

5.1.4.4 建立風險管理，執行風險管理。

5.1.4.5 建立安全事件緊急應變暨復原措施。

5.1.4.6 執行稽核改善建議事項。

5.1.4.7 執行預防措施之改善。

5.1.4.8 研討新資通安全產品或技術。

5.1.4.9 執行資通安全委員會決議事項。

5.1.4.10鑑別資通安全相關之法規。

5.1.5 緊急處理小組：由資安長指派人員組成，權責及作業內容分述如下：

5.1.5.1 當重大資通安全事件發生時，負責通報應變，並聯絡召集緊急處理小組。

5.1.5.2 協調及督導各關鍵業務流程負責人執行作業，並協調資源之調派使用。

5.1.5.3 依據事件評估之結果，得依現況建請資安長決議是否宣布災變並啟動復原作業。

5.1.5.4 當災變發生時，配合救災單位負責搶救人員、物資與設備等，以及現場指揮工作。

5.1.5.5 負責災後協調、指揮清理災害現場。

5.1.5.6 負責規劃原營運場所之現場復原工作。

5.1.6 資通安全稽核小組：由資安長指派，負責評估資通安全管理執行情形。

5.1.6.1 擬定資通安全內部稽核計畫。

5.1.6.2 執行資通安全內部稽核。

5.1.6.3 撰寫資通安全內部稽核報告。

5.1.6.4 追蹤不符合事項之改善執行情形。

5.2 管理審查會議

5.2.1 資通安全委員會應每年至少召開一次管理審查會議，必要時得召開臨時會議。

5.2.2 管理審查會議審查內容建議如下：

5.2.2.1 資通安全稽核結果及建議改善事項。

5.2.2.2 上級指導單位、內部同仁及外部單位等利害相關團體的建議。

5.2.2.3 新資通安全產品或技術導入之審查。

5.2.2.4 矯正及預防措施檢討。

5.2.2.5 風險評鑑適切性審查。

5.2.2.6 前次管理審查會議決議執行狀況。

5.2.2.7 影響資通安全管理之任何變更事項。

5.2.2.8 資通安全組織成員所提出之改善建議。

5.2.2.9 資通安全目標執行狀況報告。

本校依據「資通安全政策」所列之範圍及目標制定「目標值有效性量測表」，並以該量測結果做為評估本校資通安全目標達成情形。

5.2.2.10委外廠商查核暨自我檢核項目表、委外廠商資安管理作業自評表及委外服務案需求規格書之資安條款、資安能力要求項目之適切性。

5.2.3 管理審查會議之結論建議如下：

5.2.3.1 資通安全管理執行之各項改進措施。

5.2.3.2 更新風險評鑑與風險改善計畫。

5.2.3.3 針對可能影響資通安全管理之內、外部事件，修正資通安全管理流程與控制措施，包括：

5.2.3.3.1 營運需求的變更。

5.2.3.3.2 安全需求的變更。

5.2.3.3.3 影響現行營運需求的業務程序變更。

5.2.3.3.4 管理或法規需求的變更。

5.2.3.3.5 契約要求的變更。

5.2.3.3.6 可接受風險等級或標準的變更。

5.2.3.4 針對資通安全管理之需要，協調所需之資源。

5.2.3.5 控制措施有效性評量方式的改善。

5.2.3.6 應每年檢視「目標值有效性量測表」之量測結果與執行情形，並檢討量測項目與目標水準是否需進行調整之必要，做成改善決議。

6 相關文件

6.1 資通安全政策

6.2 資通安全組織成員表

6.3 目標值有效性量測表

附件2之附錄1

國立苑裡高級中學-資通安全組織					
文件編號	NYLSH-ISMS-01-002	機密等級	限閱	版次	4.0

目標值有效性量測表

量測項目	目標值	量測方式	量測結果	說明
114年社交工程郵件開啟率	≤10%	每年社交工程郵件演練開啟比率	■符合 □不符合，____	全年開啟比率8.5%
114年社交工程郵件點閱率	≤6%	每年社交工程郵件演練點閱比率	■符合 □不符合，____	全年點閱比率4.3%
114年社交工程郵件附件開啟率	≤2%	每年社交工程郵件演練附件開啟比率	□符合 ■不符合，____	全年附件開啟比率4.3%
114年資通安全教育訓練完成率	100%	每人每年完成教育訓練時數	■符合 □不符合，____	人員教育訓練簽到單、研習證明
備份資料回復測試	1次/年	針對非核心且對外服務之資通系統，每年辦理一次備份資料回復測試紀錄		備份資料回復測試紀錄

附件3

國立苑裡高級中學-資通安全組織					
文件編號	NYLSH-ISMS-01-003	機密等級	限閱	版次	4.0

國立苑裡高級中學資通安全組織成員表

職務	職稱	分機	電子郵件
資通安全委員會			
資安長	校長	100	ylsh100@ylsh.mlc.edu.tw
委員	教務主任	200	ylsh200@ylsh.mlc.edu.tw
委員	學務主任	300	ylsh300@ylsh.mlc.edu.tw
委員	總務主任	500	ylsh500@ylsh.mlc.edu.tw
委員	輔導主任	400	ylsh400@ylsh.mlc.edu.tw
委員	圖書館主任	800	ylsh800@ylsh.mlc.edu.tw
委員	人事主任	700	ylsh700@ylsh.mlc.edu.tw
委員	主計主任	600	ylsh600@ylsh.mlc.edu.tw
委員	秘書	101	ylsh101@ylsh.mlc.edu.tw
資通安全小組			
資安執行秘書	圖書館主任	800	ylsh800@ylsh.mlc.edu.tw
組長(由資安執行秘書擔任)	主任	800	ylsh800@ylsh.mlc.edu.tw
資安承辦人	組長	801	ylsh801@ylsh.mlc.edu.tw
組員	資訊專長教師	808	mhchen@ylsh..mlc.edu.yw
資通安全稽核小組			
組長	秘書	101	ylsh101@ylsh.mlc.edu.tw
組員	人事主任	700	ylsh700@ylsh.mlc.edu.tw
組員	具稽核專長之專業人員	外聘	

國立苑裡高級中學-資通安全組織成員表					
文件編號	NYLSH-ISMS-01-003	機密等級	限閱	版次	4.0

緊急處理小組			
組長	主　　任	800	ylsh800@ylsh.mlc.edu.tw
組員	資訊媒體組長	801	ylsh801@ylsh.mlc.edu.tw
組員	圖書館館員	802	ylsh802@ylsh.mlc.edu.tw

學校總機：(037) 868680

附件4

國立苑裡高級中學-保密切結書					
文件編號	NYLSH-ISMS-01-004	機密等級	限閱	版次	4.0

保密切結書

本人 _____ 將嚴守工作保密規定與國家相關法令，對業務機密負完全保密之責，並尊重智慧財產權。絕不擅自洩漏、傳播職務上任何業務相關資料及任職期間經辦、保管或接觸之所有須保密訊息資料；絕不擅自複製、傳播任何侵害智慧財產權之任何程式、軟體。保密之義務，不因調職或離職而終止。如有違反，依法負刑事、民事及行政責任。

此致

國立苑裡高級中學

立 同 意 書 人：

身 分 證 字 號之前6碼：

電　　話：

地　　址：

中　　華　　民　　國　　年　　月　　日

附件5

國立苑裡高級中學-經費配置表					
文件編號	NYLSH-ISMS-01-005	機密等級	限閱	版次	4.0

國立苑裡高級中學經費配置表

填表日期：115 年 7 月 15 日

經費類別	單位(元)
114年機關預算執行	
114年機關年度**預算**執行情形-資本門	8,197,238
114年機關年度**預算**執行情形-經常門	212,574,816
114年機關年度預算執行情形-小計	**220,772,054**
114年度**資訊**預算執行情形-資本門	2,996,879
114年度**資訊**預算執行情形-經常門	834,163
114年度資訊預算執行情形-小計	**3,831,042**
114年度**資安**預算執行情形-資本門	55,000
114年度**資安**預算執行情形-經常門	256,500
114年度資安預算執行情形-小計	**311,500**
資訊預算佔機關年度預算比例	0.017352
資安預算佔資訊預算比例	0.081309

主計單位	承辦人		主管		資安長	
資通安全小組	承辦人		主管			

註：依據數位發展部資通安全署資通安全作業管考系統(https://spm.nat.gov.tw/Account/Login)，

1. 資訊經費係指各機關之業務費、設備及投資費：

(1). 業務費（經常門）：教育訓練費、資訊服務費，如凡公務所需使用資訊操作、維修、購買雲端等服務費用、金額未達1萬元之軟體購置或屬營業租賃性質之資訊設備租金屬之。

(2). 設備及投資(資本門)：資訊軟硬體設備費，如凡公務所需各項電腦設施、週邊設備、裝置（含一次購買時所配置 之套裝軟體，如作業系統軟體，以及後續2年以上效益之軟體改版、升級與應用系統開發規 劃設計）及雲端服務等購置（含資本租賃）費用屬之。

2. 資安經費(經常門、資本門)：辦理資通安全管理法及其子法之法遵事項相關經費。

附件6

國立苑裡高級中學-資通資產管理					
文件編號	NYLSH-ISMS-01-005	機密等級	限閱	版次	4.0

1 目的

建立國立苑裡高級中學（以下簡稱本校）資通資產管理，訂定資通資產分類、分級、價值評估、標示及處理之遵循原則，並據以辦理各項資通資產管理作業，避免因人為疏失、蓄意或自然災害等風險所造成之傷害。

2 適用範圍

本校承辦相關資訊業務作業流程之資通資產。

3 權責

3.1 資安執行秘書：負責定期審議「資通資產盤點表」及價值評估結果，並督導相關活動之進行。

3.2 資通安全小組：負責定期辦理資通資產異動調查與彙整，提供最新之「資通資產盤點表」，並呈報資通安全委員會。

3.3 資通資產權責單位：負責所管轄內資通資產之存取授權，並評估與審核資通資產分類分級及價值之結果，得另指定資通資產保管單位。

3.4 資通資產保管單位：對於指定資通資產，具有落實資通資產權責單位所委託之保護管理責任。

3.5 資通資產使用單位：對於資通資產之使用，必須依據權責單位要求，並具有正確使用操作之責任。

4 名詞定義

4.1 機密性（Confidentiality）：確保只有經授權的人，才可以存取資訊。

4.2 完整性（Integrity）：確保資訊與處理方法的正確性與完整性。

4.3 可用性（Availability）：確保經授權的使用者在需要時可以取得資訊及相關資產。

4.4 資通資產權責單位：對該項資通資產具有判斷資產價值、決定存取權限或新增、刪除、修改權限之單位，同時也是資通資產的擁有單位。

4.5 資通資產保管單位：依據權責單位之需求標準，執行資通資產日常保護、異動與維護之執行單位。

4.6 資通資產使用單位：因業務需求，經授權可直接或間接使用該資通資產之單位。

5 作業說明

5.1 資通資產鑑別

5.1.1 各資通資產權責單位應鑑別所管轄之資通資產，並建立「資通資產盤點表」。

5.1.2 各資通資產權責單位應定期更新與維護所管轄之資通資產盤點表。

5.1.3 資通資產盤點表由各權責單位提供，資通安全小組負責彙整，並陳報至資通安全委員會，以確保資通資產編號及清單之完整性。

5.2 資通資產分類

5.2.1 資通資產依其性質不同，分為 7 類：人員、文件、軟體、通訊、硬體、資料、環境。

5.2.1.1 人員（People/PE)：包含全體同仁，以及委外廠商。

5.2.1.2 文件（Document/DC)：以紙本形式存在之文書資料、報表等相關資訊，包含公文、列印之報表、表單、計畫等紙本文件。

5.2.1.3 軟體（Software/SW)：作業系統、應用系統程式、套裝軟體等，包含原始程式碼、應用程式執行碼、資料庫等。

5.2.1.4 通訊（Communication/CM)：網通設備、WiFi AP、網路電話、網路安全設備、提供資訊傳輸、交換之線路或服務。

5.2.1.5 硬體（Hardware/HW)：主機設備等相關硬體設施，如印表機、電子看板、儲存設備。

5.2.1.6 資料（Data/DA）：儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊。

5.2.1.7 環境（Environment/EV）：相關基礎設施及服務，包含辦公室實體、實體機房、電力、消防設施、網路攝影機、門禁系統等。

5.2.2 各類資通資產機密等級分為 4 級：一般、限閱、敏感、機密。各等級之評估標準如下：

5.2.2.1 一般：無特殊之機密性要求，可對外公開之資訊。

5.2.2.2 限閱：僅供組織內部人員或被授權之單位及人員使用。

5.2.2.3 敏感：僅供組織內部相關業務承辦人員及其主管，或被授權之單位及人員使用。

5.2.2.4 機密：為組織、主管機關或法律所規範之機密資訊。

5.2.3 資通資產之機密等級應定期審核，視實際需要予以調整。

5.2.4 不同等級之資通資產合併使用或處理時，以其中最高之等級為機密等級。

5.3 資通資產價值鑑別

5.3.1 資通資產權責單位應鑑別其所管轄內所有資通資產之價值。

5.3.2 資通資產價值除考量資通資產機密等級之外，尚需考量資通資產之可用性及完整性，其評估標準如下：

5.3.2.1 機密性評估標準

評估標準	數值
此資通資產無特殊之機密性要求	1
此資通資產僅供組織內部人員或被授權之單位及人員使用	2
此資通資產僅供組織內部相關業務承辦人員及其主管，或被授權之單位及人員使用	3
此資通資產含有組織或法律所規範的機密資訊	4

5.3.2.2 完整性評估標準

評估標準	數值
該資通資產本身完整性要求極低	1
該資通資產本身具有完整性要求，當完整性遭受破壞時，不會對組織造成傷害	2
該資通資產具有完整性要求，當完整性遭受破壞時會對組織造成傷害，但不至於太嚴重	3
該資通資產具有完整性要求，當完整性遭受破壞時會對組織造成傷害，甚至造成業務終止	4

5.3.2.3 可用性評估標準

評估標準	數值
該資通資產可容許失效3工作天以上	1

該資通資產可容許失效8工作小時以上，3工作天以下	2
該資通資產僅容許失效4工作小時以上，8工作小時以下	3
該資通資產僅容許失效4工作小時以下	4

5.3.2.4 資通資產價值之決定將依據資通資產之機密性、完整性及可用性評估之後，取 3 者之最大值以為資通資產之價值。

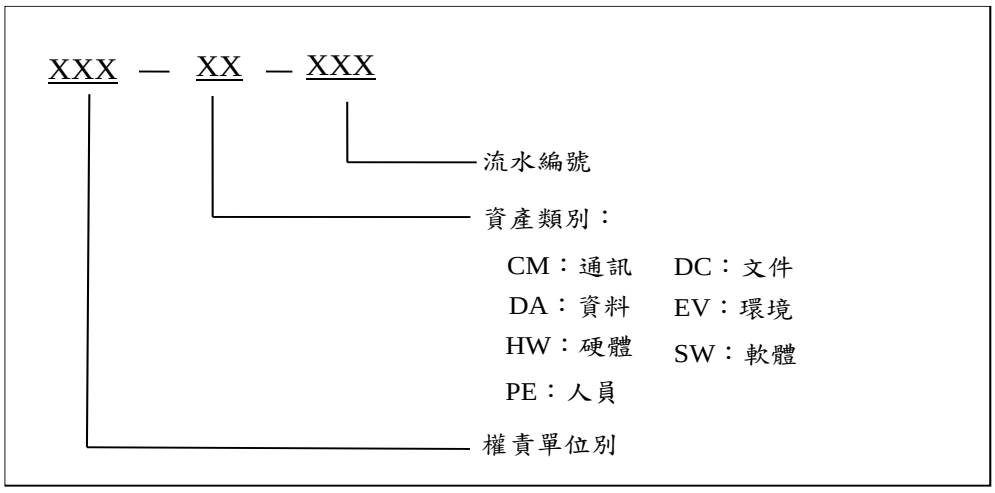
5.4 資通資產盤點表及價值確認

5.4.1 資通資產權責單位應依據資通資產盤點表之機密性、可用性及完整性之評估標準，確認資產價值。

5.4.2 資通資產盤點表及價值評估結果，應呈報資通安全委員會審議。

5.5 資通資產編號及標示

5.5.1 第 1~3 碼為權責單位別，第 4~5 碼為資產類別，第 6~8 碼為資通資產流水編號。



資通資產編碼方式圖

5.5.2 已列入機密等級分類的資通資產，應明確標示其機密等級，避免其機密性遭破壞。

5.5.3 實體設備之重要等級標示方式：

5.5.3.1 實體設備之重要等級應以不同顏色標籤區分（資產價值2為綠色標籤，資產價值3為黃色標籤，資產價值4為藍色標籤）。

5.5.3.2 文件之機密等級應於文件封面做明確的標示。系統輸出機密等級為敏感以上的報表，如系統未自動標示，則由資通資產權責單位做額外的明顯註記。

5.6 資通資產管理作業

5.6.1 資通資產異動管理，如：新增、刪除、修改等控管原則，請參閱「資通資產異動作業」，如附件8。

5.7 覆核

5.7.1 權責單位每年至少進行一次資產盤點與資通資產盤點表覆核，以更新及確保資通資產盤點表的正確性及完整性。

5.7.2 當範圍內有以下的狀況發生時，則實施不定期的覆核，以更新及確保資通資產盤點表的正確性及完整性。

5.7.3 有新增、變更或移除資通資產。

5.7.4 系統有重大異動。

5.7.5 作業環境改變。

5.8 資通資產之報廢

5.8.1 資通資產之報廢或銷毀，應依據「資通資產異動作業」，採取適當之方式進行銷毀。

5.9 資通資產之處理規範

5.9.1 針對價值 3 或 4 之資通資產，應加強安全保護及存取控制管控措施，以防止洩漏或不法及不當的使用。

5.9.2 價值 3 或 4 文件類資通資產之安全處理應符合以下作業要求：

5.9.2.1 紙類文件不再使用時，應銷毀處理。

5.9.2.2 系統流程、作業流程、資料結構及授權程序等系統相關文件，應予適當保護，以防止不當利用。

5.9.2.3 系統文件應指定專人管理，並鎖在安全的儲櫃或其他安全場所，且發送對象應以最低必要的人員為限。

5.9.2.4 電腦產製的文件，應與其應用檔案分開存放，且應建立適當的存取保護措施。

5.9.3 價值 3 或 4 軟體類資通資產之安全處理作業，請參閱「存取控制管理」，如附件 9 及「系統開發與維護」，如附件 12。

5.9.4 價值 3 或 4 硬體類資通資產之安全處理作業，請參閱「實體安全管理」，如附件 10。

5.9.5 應定期檢討價值 3 或 4 之資通資產盤點表內容，以確保重要資產受到適當的安全保護。

6 相關文件及網站

6.1 存取控制管理

6.2 系統開發與維護

6.3 實體安全管理

6.4 資通資產異動作業

6.5 資通資產盤點表

6.6 國立中興大學計算機及資訊網路中心製「資安風險評鑑方法論」，說明資訊資產分類原則及資訊資產分級標準（網址：https://youtu.be/01JAIgkpSgo?t=190）。

6.7 國立中興大學之資訊資產詳細風險評鑑（網址：https://sites.google.com/email.nchu.edu.tw/ssdlc/ra2）。

附件6之附錄1

國立苑裡高級中學-資通資產管理					
文件編號	NYLSH-ISMS-01-006	機密等級	限閱	版次	4.0

國立苑裡高級中學資通資產盤點表

資產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	使用單位	機密性	完整性	可用性	資產價值
LIB-CM-001	CM	防火牆	FortiGate 201E	圖書館	圖書館	圖書館	1	2	3	3
LIB-CM-002	CM	骨幹集線器	Extreme X620-16x	圖書館	圖書館	圖書館	1	1	3	3
LIB-CM-003	CM	交換式集線器	Extreme X440G2	圖書館	圖書館	圖書館	1	1	2	2
LIB-CM-004	CM	網路環境	實體線路	圖書館	圖書館	圖書館	1	1	2	2
LIB-CM-005	CM	核心交換器	Csico C9300-TA	圖書館	圖書館	圖書館	1	1	3	3
LIB-CM-006	CM	中繼網路交換器	Aruba 1930 48G 4SFP+	圖書館	圖書館	圖書館	1	1	2	2
LIB-CM-007	CM	邊際網路交換器	C1300-24FP-4X	圖書館	圖書館	圖書館	1	1	2	2

國立苑裡高級中學-資通資產管理					
文件編號	NYLSH-ISMS-01-006	機密等級	限閱	版次	4.0

資產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	使用單位	機密性	完整性	可用性	資產價值
LIB-EV-001	EV	穩壓器	盛景電子	圖書館	圖書館	圖書館	1	1	1	1
LIB-EV-002	EV	不斷電系統	飛瑞、APC	圖書館	圖書館	圖書館	1	1	1	1
LIB-EV-003	EV	機房	資源中心大樓4F	圖書館	圖書館	圖書館	1	2	3	3
GEN-SW-001	SW	公文管理系統	帝緯	總務處	總務處	總務處	2	2	3	3
GEN-SW-002	SW	財產管理系統	慧二	總務處	總務處	總務處	2	2	3	3
GEN-SW-003	SW	薪資出納管理	艾富	總務處	總務處	總務處	2	2	3	3
GEN-EV-004	EV	消房設施	消房設備	總務處	總務處	總務處	1	1	2	2
LIB-DC-001	DC	資安管理文件	ISMS 相關文件	圖書館	圖書館	圖書館	2	2	2	2
LIB-SW-001	SW	作業系統	Windows Server	圖書館	圖書館	圖書館	2	1	2	2
LIB-SW-002	SW	學校網站	WordPress 7.0.1	圖書館	圖書館	圖書館	2	2	3	3

資產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	使用單位	機密性	完整性	可用性	資產價值
LIB-SW-003	SW	DNS 作業系統	ubuntu	圖書館	圖書館	圖書館	1	3	3	3
LIB-SW-004	SW	圖書管理系統	寶慶圖書有限公司	圖書館	圖書館	圖書館	1	2	2	2
LIB-HW-001	HW	VM主機	HP ProLiant DL380 Gen9	圖書館	圖書館	圖書館	2	3	3	3
LIB-HW-002	HW	VM 主機2備援	HP ProLiant DL380 Gen8	圖書館	圖書館	圖書館	2	3	2	3
LIB-PE-001	PE	系統維護廠商	晉暘資訊公司	圖書館	圖書館	圖書館	2	2	1	2
LIB-PE-002	PE	系統管理人員	圖書館主任、資媒組長	圖書館	圖書館	圖書館	2	2	1	2
LIB-PE-003	PE	系統使用人員	有使用權限之人員(E-mail、Web)	圖書館	圖書館	圖書館	2	2	1	2
PER-SW-001	SW	雲端差勤系統	宏權資訊	人事室	人事室	人事室	2	3	3	3

國立苑裡高級中學-資通資產管理					
文件編號	NYLSH-ISMS-01-006	機密等級	限閱	版次	4.0

資產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	使用單位	機密性	完整性	可用性	資產價值
ACA-SW-002	SW	排課系統	欣河校務行政系統	教務處	教務處	教務處	1	1	2	2
ACA-SW-003	SW	校務系統(含學習歷程)	亞昕校務行政系統	教務處	教務處	教務處	4	4	4	4
ACA-PE-001	PE	系統維護廠商	亞昕資訊	教務處	教務處	教務處	2	2	3	3
ACA-PE-002	PE	系統操作人員	業務相關人員	教務處	教務處	教務處	1	1	1	1
ACA-PE-003	PE	系統維護人員	具權限者	教務處	教務處	教務處	2	2	2	2
ACA-DA-001	DA	學籍資料	學生學籍資料	教務處	教務處	教務處	4	4	4	4
ACA-EV-001	EV	辦公室環境	教務處辦公室	教務處	教務處	教務處	1	1	1	1
ACA-DC-001	DC	辦公室文件	教務處公務相關文件	教務處	教務處	教務處	1	1	1	1

使用單位	承辦人		主管	

資通資產價值為4者，須會辦資通安全小組

資通安全小組	承辦人		主管	

附件7

國立苑裡高級中學-風險評鑑與管理					
文件編號	NYLSH-ISMS-01-007	機密等級	限閱	版次	4.0

1 目的

建立國立苑裡高級中學（以下簡稱本校）風險評鑑與管理，提供本校資通資產之權責單位、保管單位，以及使用單位，共同遵行之風險評鑑標準，有效執行風險控管，預防資通安全事件之威脅。

2 適用範圍

本校承辦相關資通業務作業流程之風險管理。

3 權責

3.1 資通安全委員會：

負責可接受風險值、風險評鑑結果、風險改善計畫與控制措施之審查及核定。

3.2 資通安全小組：

負責相關資通資產風險評鑑結果之複核，並針對超過可接受風險值之項目提出建議之控管措施，並產出風險改善計畫。

3.3 權責單位主管：

負責所屬單位業務範圍之風險評鑑結果審核作業。

3.4 資通資產權責單位：

負責執行資通資產之威脅與弱點評估、風險值計算等程序項目。

4 名詞定義

4.1 機密性(Confidentiality)：確保只有經授權的人，才可以存取資訊。

4.2 完整性(Integrity)：確保資訊與處理方法的正確性與完整性。

4.3 可用性(Availability)：確保經授權的使用者在需要時可以取得資訊及相關資產。

4.4 可接受風險值：各類資訊資產之最低風險容忍度。

4.5 殘餘風險（Residual Risk）：在採用相關控制措施之後剩餘的風險。

4.6 威脅（Threat）：可能對系統或組織造成傷害之意外事件。

4.7 弱點（Vulnerability）：因資通資產本身狀況或所處環境之下，可能受到威脅利用而造成資產受到損害之因子。

4.8 風險（Risk）：可能對團體或組織的資產發生損失或傷害的潛在威脅，通常利用弱點所產生之影響及發生可能性來衡量。

5 作業說明

5.1 鑑別資產

5.1.1 資通資產之鑑別應依據「資通資產管理」進行風險鑑別及分類。

5.2 鑑別風險

5.2.1 威脅及弱點評估：可參考 ISO 27005 將各類資通資產可能面臨之威脅與弱點項目，以建立「威脅及弱點評估表」。

5.2.2 可能的威脅、弱點項目：參考國立華南高級商業職業學校及國立中興大學計算機及資訊網路中心之「資訊資產威脅及弱點評估表」列表以下範列。

5.2.2.1 人員（People/PE）可能的威脅、弱點項目。

威脅	弱點	風險改善建議措施
人員可利用性的違反	缺乏人員	加強人員教育訓練及控管
設備或媒體的破壞	不充分的招募程序	加強人員教育訓練及控管
使用上的誤用	不足的安全訓練	加強人員教育訓練及控管
使用上的誤用	不正確的使用硬體和軟體	加強人員教育訓練及控管
使用上的誤用	欠缺安全認知	加強人員教育訓練及控管
非法的處理資料	欠缺監控機制	加強人員教育訓練及控管
媒體或文件的盜竊	外部或清潔人員未經監督的工作	加強人員教育訓練及控管
未經授權的使用設備	欠缺正確使用電信媒體和訊息的政策	加強人員教育訓練及控管

5.2.2.2 文件（Document/DC）可能的威脅、弱點項目。

威脅	弱點
故意的破壞	人員安全訓練不足
	建築物、房間的實體進出控制不足
	缺乏安全警覺
	識別與認證機制的不足
遺失	人員安全訓練不足
	缺乏適當管理機制
失竊	人員安全訓練不足
	外部人員缺乏人員陪同作業
	存取權限授與不當
	資料銷毀時的不注意
操作人員的錯誤	不正確的使用軟體和硬體
	文件化管理之缺乏或不足

威脅	弱點
	缺乏安全警覺
	缺乏資料、程式、文件備份
	缺乏監督監督機制
	專業訓練不足

5.2.2.3 軟體（Software/SW）可能的威脅、弱點項目。

威脅	弱點	風險改善建議措施
濫用權限	無或不充分的軟體測試	建立軟體使用及檢查機制
	軟體上知名的缺點	建立軟體使用及檢查機制
	離開工作站時未確實登出	建立軟體使用及檢查機制
	處置或再使用儲存媒體未適當地消磁	建立軟體使用及檢查機制
	欠缺稽核軌跡	建立軟體使用及檢查機制
	錯誤的存取權限分配	建立軟體使用及檢查機制
資料的訛用	廣泛散佈的軟體	建立軟體使用及檢查機制
	在時間方面將應用系統程式應用至錯誤的資料	建立軟體使用及檢查機制
使用上的誤用	複雜的使用者介面	建立使用者手冊及規定
	欠缺文件	建立使用者手冊及規定
	不正確的參數設定	建立使用者手冊及規定
	不正確的日期	建立使用者手冊及規定
偽造權限	欠缺像使用者授權的識別與授權機制	建立使用者管理機制
	未保護的通行碼	建立使用者管理機制

	不良的通行碼管理	建立使用者管理機制
非法的處理資料	啟動不必要的服務	建立軟體使用及檢查機制
軟體機能失常	不成熟或新的軟體	建立軟體獲取檢查機制
	對開發者不清楚或未完成的規格	建立軟體獲取檢查機制
竄改軟體	欠缺有效的變更控制	建立軟體獲取檢查機制
	未控制的下載與使用軟體	建立軟體獲取檢查機制
	欠缺備份複本	建立軟體獲取檢查機制
媒體或文件的盜竊	欠缺對建築物、門窗的實體保護	建立實體控制機制
未經授權的使用設備	未能產出管理報告	建立實體控制機制

5.2.2.4 通訊（Communication/CM）可能的威脅、弱點項目。

威脅	弱點
線路中斷	連線電纜失效
失效	不正確的使用軟體和硬體
	缺乏適當的維護工作
	缺乏有效變更控制
	缺乏硬體耗損控管
	專業訓練不足
	缺乏監督機制
未經授權使用者的網路存取	外部人員缺乏人員陪同作業
	建築物、房間的實體進出控制的不足

5.2.2.5 硬體（Hardware/HW）可能的威脅、弱點項目。

威脅	弱點	風險改善建議措施
危害資訊系統可維護性	儲存媒體的維護不足或錯誤安裝	建立維護機制
設備或媒體的破壞	缺乏定期更換概要	建立維護機制
灰塵、腐蝕、凍結	對濕度、灰塵、土壤的敏感性	建立環控監測機制
電磁輻射	對電磁輻射的敏感性	建立環控監測機制
使用上的誤用	缺乏有效的組態變更管理	建立變更管理機制
電力供應喪失	對電壓變化的敏感性	建立電力備援機制
氣象現象	對溫度變化的敏感性	建立環控監測機制
媒體或文件的盜竊	未保護的儲存庫	建立實體控制機制
	處置時不小心	建立實體控制機制
	未控制的複製	建立實體控制機制
否認行動	欠缺寄送或接收訊息的證明	建立不可否認性機制
偷聽	未保護的傳輸線	建立電纜線保護監控機制
	未保護的敏感性電信	建立電纜線保護監控機制
電信設備故障	不良的電纜接合	建立電纜線保護監控機制
	單點失誤	建立電纜線保護監控機制
偽造權限	欠缺寄送者或接收者的識別與授權	建立存取制機制
遠端暗中監視	不安全的網路架構	定期檢視網路架構
	以明碼傳送通行碼	建立資料傳送加密機制
資訊系統飽和	不充分的網路管理、路由的彈性	建立網路監控機制
未經授權的使用設備	未保護的公用網路連接	建立網路監控機制

5.2.2.6 資料（Data/DA）可能的威脅、弱點項目。

威脅	弱點
故意的破壞	人員安全訓練不足
	建築物、房間的實體進出控制不足
	缺乏安全警覺
	識別與認證機制的不足
遺失	人員安全訓練不足
	缺乏適當管理機制
失竊	人員安全訓練不足
	外部人員缺乏人員陪同作業
	存取權限授與不當
	資料銷毀時的不注意
操作人員的錯誤	不正確的使用軟體和硬體
	文件化管理之缺乏或不足
	缺乏安全警覺
	缺乏資料、程式、文件備份
	缺乏監督監督機制
	專業訓練不足
未適當控管儲存媒介之存取	人員安全訓練不足
	未經控管之資料複製
	存取權限授與不當
	識別與認證機制的不足
	未落實桌面淨空或螢幕鎖定
	缺乏安全警覺
	缺乏監督機制
	資料銷毀時的不注意
	機密資料的外洩
	儲存媒介內之資料沒有適當刪除就丟棄或重覆使用
	外部人員缺乏人員陪同作業

5.2.2.7 環境（Environment/EV）可能的威脅、弱點項目。

威脅	弱點	風險改善建議措施
設備或媒體的破壞	對建築物與房間不充分或草率的實體存取控制	建立實體控制機制
颱風	缺乏建築物、門、窗等物質的保護	建立實體控制機制
地震	缺乏建築物、門、窗等物質的保護	建立實體控制機制
淹水、水災	位於容易淹水、水災的區域	建立環控監測機制
漏水	沒有做好維護的工作	建立環控監測機制
	環境控制系統失效	建立環控監測機制
火災	人員安全訓練不足	建立環控監測機制
	缺乏消防器材的保護	建立環控監測機制
	儲存易燃物	建立環控監測機制
	環境控制系統失效	建立環控監測機制
停電、電力供應喪失	不穩定的供電	建立環控監測機制
	不斷電系統失效	建立環控監測機制
	發電機失效	建立環控監測機制
灰塵	容易潮濕、有灰塵、穢物	建立環控監測機制
空調失效	沒有做好維護的工作	建立環控監測機制
	維護服務回應時間過長	建立環控監測機制
	缺乏緊急應變機制	建立環控監測機制
設備的盜竊	欠缺建築物、門窗的實體保護	建立實體控制機制
濫用權限	欠缺軟體使用者註冊與撤銷註冊的正式程序	建立帳密存取控制機制
	欠缺存取權限審查監督程序	建立帳密存取控制機制
	欠缺或未充分提供安全聯絡通道	建立帳密存取控制機制
	欠缺監控資訊處理設施的正式程序	建立帳密存取控制機制
	欠缺一般的稽核、監控	建立帳密存取控制機制
	欠缺風險識別與評鑑的程序	建立帳密存取控制機制
	欠缺記錄於管理員與操作員日誌的錯誤報告	建立帳密存取控制機制
危害資訊系統可維護性	不充分的服務維護回覆	建立適當的維護機制
	欠缺或不充分的服務等級協議	建立適當的維護機制
	欠缺變更控制程序	建立適當的維護機制
資料的訛用	欠缺文件控制程序	建立文件控制及監督之程序

威脅	弱點	風險改善建議措施
	欠缺記錄監督程序	建立文件控制及監督之程序
來自不可信賴來源的資料	欠缺公開資訊授權程序	建立公開資訊審核機制
否認行動	欠缺資訊安全職責的適當配置	建立不可否認性機制
設備故障	欠缺持續計畫	建立設備故障復原之機制
使用上的誤用	欠缺電子郵件使用政策	建立電子郵件使用機制
	欠缺引進軟體至業務系統的程序	建立軟體使用及控管機制
	欠缺管理員與操作員日誌的記錄	建立日誌紀錄機制
	欠缺機密資訊處理的程序	建立機密資訊處理之程序
	欠缺在工作說明的資訊安全職責	加強人員教育訓練
非法的處理資料	欠缺或未充分提供安全處理	建立安全提供資料及聯絡機制
設備的盜竊	欠缺已定義的資訊安全事故懲戒程序	建立資安事故相關獎懲程序
	欠缺行動電腦使用的正式政策	建立行動電腦使用之管理機制
	欠缺場所外資產的控制	建立資訊資產進出管理之機制
媒體或文件的盜竊	欠缺或不充分桌面淨空和螢幕淨空	建立桌面淨空之機制
	欠缺資訊處理設施的授權	建立實體控制機制
	欠缺已建立的安全危害監控機制	建立實體控制機制
未經授權的使用設備	欠缺一般的管理階層審查	建立管理階層審查機制
	欠缺通報安全弱點的程序	建立完整資通安全通報機制
使用偽造或複製的軟體	欠缺遵循智慧財產權規定的程序	建立軟體使用及控管機制

5.2.3 事件發生機率與影響程度評估如下：

5.2.3.1 威脅的等級對應評估標準

評估標準	評估值
威脅發生之可能性為低	1
威脅發生之可能性為中	2
威脅發生之可能性為高	3

5.2.3.2 弱點的等級對應評標標準

評估標準	評估值
該弱點不容易被威脅利用	1
該弱點容易被威脅利用	2
該弱點非常容易被威脅利用	3

5.2.4 風險值的計算

評估威脅發生之可能性及弱點受到威脅利用之容易度，計算出風險值。

風險值=（資通資產價值 × 威脅等級 × 弱點等級）

5.2.5 事件風險權值對照

威脅等級（發生之可能性）		低(1)			中(2)			高(3)		
弱點等級（受到威脅利用之容易度）		低(1)	中(2)	高(3)	低(1)	中(2)	高(3)	低(1)	中(2)	高(3)
資產價值	1	1	2	3	2	4	6	3	6	9
	2	2	4	6	4	8	12	6	12	18
	3	3	6	9	6	12	18	9	18	27
	4	4	8	12	8	16	24	12	24	36

5.3 風險管理

5.3.1 可接受風險值的決定

5.3.1.1 資通資產之可接受風險值，需經資通安全委員會開會決議，並記載於會議紀錄中。

5.3.1.2 資通安全委員會每年召開會議檢討可接受風險值。可接受風險必須考量組織環境及作業之安全需求，並進行適當地調整。

5.3.1.3 資通安全小組應針對高於可接受風險值項目，產出「風險評鑑彙整暨改善計劃表」作為風險管理之依據。

5.3.2 選擇控制措施

5.3.2.1 超出可接受風險值之項目，應選擇適當之控管措施，並填寫「風險評鑑彙整暨改善計劃表」，說明風險控管措施之執行辦法。

5.3.2.2 「風險評鑑彙整暨改善計劃表」應陳報資通安全委員會開會審核，並列入追蹤管理程序。

5.3.3 風險改善狀況的後續追蹤

5.3.3.1 資通安全小組應針對「風險評鑑彙整暨改善計劃表」彙整控管，持續追蹤至完成改善為止。

5.3.3.2 應於各項風險改善措施完成後，應進行風險再評鑑，以確保相關改善措施的有效性。

5.4 覆核

5.4.1 監控

控制措施的實施必須建立相對應的指標或紀錄，以反應出控制措施實施的狀況及成效，便於管理階層及相關人員做定期或不定期審視。

5.4.2 持續改善

為保持本風險評鑑方法之有效性與適用性，資通安全小組得定期檢討可接受風險值與「威脅及弱點評估表」之項目。以期確保資通資產均處於最佳保護之下，提供持續不中斷的營運。

5.4.3 風險重新評鑑

5.4.3.1 每年應至少執行一次風險評鑑。

5.4.3.2 當有新增系統、系統有重大異動或作業環境改變時則應執行不定期之風險評鑑。

6 相關文件及網站

6.1 資通資產管理

6.2 威脅及弱點評估表

6.3 風險評鑑彙整暨改善計劃表

6.4 國立中興大學計算機及資訊網路中心之「資訊資產威脅及弱點評估表」：共同開發者為教育機構資安驗證中心、中興大學計算機及資訊網路中心、中興大學前瞻無所不在商務實驗室、屏東大學數位應用資訊安全實驗室、品科技（網址：https://sites.google.com/email.nchu.edu.tw/ssdlc/ra2）。

附件7之附錄1

國立苑裡高級中學-風險評鑑與管理					
文件編號	NYLSH-ISMS-01-007	機密等級	限閱	版次	4.0

國立苑裡高級中學威脅及弱點評估表

資產編號	資產類別	資產名稱	資產價值	威脅	弱點	威脅等級	弱點等級	風險值
LIB-CM-001	CM	防火牆	3	天然災害	實體故障	1	3	9
LIB-CM-002	CM	骨幹集線器	3	天然災害	實體故障	1	2	6
LIB-CM-003	CM	交換式集線器	3	天然災害	實體故障	1	2	6
LIB-CM-004	CM	網路環境	3	天然災害	實體故障	1	3	9
LIB-CM-005	CM	核心交換器	3	天然災害	實體故障	1	4	12
LIB-CM-006	CM	中繼網路交換器	3	天然災害	實體故障	1	4	12
LIB-EV-001	EV	穩壓器	4	天然災害	實體故障	1	3	12
LIB-EV-002	EV	不斷電系統	4	天然災害	實體故障	1	1	4
LIB-EV-003	EV	機房	4	天然災害	實體故障	1	3	12

附件7之附錄1

國立苑裡高級中學-風險評鑑與管理					
文件編號	NYLSH-ISMS-01-007	機密等級	限閱	版次	4.0

資產編號	資產類別	資產名稱	資產價值	威脅	弱點	威脅等級	弱點等級	風險值
GEN-EV-004	EV	消房設施	4	天然災害	實體故障	1	1	4
LIB-DC-001	DC	資安管理文件	3	技術因素	邏輯因素	1	3	9
LIB-SW-001	SW	作業系統	4	技術因素	系統失效	1	3	12
LIB-SW-002	SW	網頁管理系統	3	技術因素	系統失效	1	2	6
LIB-SW-003	SW	DNS 作業系統	4	技術因素	系統失效	1	2	8
LIB-HW-001	HW	VM 主機	3	技術因素	實體故障	2	2	12
LIB-HW-002	HW	VM 主機2備援	4	技術因素	實體故障	1	3	12
LIB-PE-001	PE	系統維護廠商	2	人為因素	人員控管	1	2	4
LIB-PE-002	PE	系統管理人員	2	人為因素	人員控管	1	1	2
LIB-PE-003	PE	系統使用人員	2	人為因素	人員控管	1	1	2

附件7之附錄1

國立苑裡高級中學-風險評鑑與管理					
文件編號	NYLSH-ISMS-01-007	機密等級	限閱	版次	4.0

資產編號	資產類別	資產名稱	資產價值	威脅	弱點	威脅等級	弱點等級	風險值
ACA-SW-003	SW	校務系統	4	人為因素	系統失效	1	3	12
ACA-SW-004	SW	學生學習歷程系統	4	人為因素	系統失效	1	1	4
ACA-PE-001	PE	系統維護廠商	2	人為因素	人員控管	1	2	4
ACA-PE-002	PE	系統操作人員	2	人為因素	人員控管	1	2	4
ACA-PE-003	PE	系統維護人員	2	人為因素	人員控管	1	2	4
ACA-DA-001	DA	學籍資料	4	人為因素	邏輯因素	1	3	12
ACA-EV-001	EV	辦公室環境	4	天然災害	實體故障	1	2	8
ACA-DC-001	DC	辦公室文件	3	人為因素	邏輯因素	1	2	6

附件7之附錄2

國立苑裡高級中學-風險評鑑與管理					
文件編號	NYLSH-ISMS-01-007	機密等級	限閱	版次	4.0

國立苑裡高級中學風險評鑑彙整暨改善計劃表

項次	資產編號	資產類別	資產名稱	資產說明	權責單位	資產價值	風險事件		風險值	風險改善建議措施	預計改善時間與處理方式	負責人員	風險再評估			
							威脅	弱點					資產價值	威脅等級	弱點等級	風險值
1	LIB-EV-002	EV	不斷電系統	飛瑞、APC	資媒組	4	天然災害	實體故障	2	定期保養、維護	請維護廠商定期保養維護	資媒組	4	2	2	16
2	LIB-HW-001	HW	VM 主機	HP DL380 Gen9	資媒組	3	技術因素	實體故障	3	定期保養、更新主機	請維護廠商定期保養維護	資媒組	3	2	2	12

附件8

國立苑裡高級中學-資通資產異動作業					
文件編號	NYLSH-ISMS-01-008	機密等級	限閱	版次	4.0

1 目的

建立保護國立苑裡高級中學（以下簡稱本校）之資通資產於新增、異動、報廢時，能依據適當之程序，進行安全可靠之處置。

2 適用範圍

本校承辦相關資通業務之資通資產新增、異動、報廢作業。

3 權責

本校相關人員、約聘（僱）人員與工讀生，確實執行資通資產新增、異動、報廢作業之程序。

4 名詞定義

無。

5 作業說明

5.1 資通資產之新增、異動

5.1.1 資通資產新增或異動時，資通資產使用單位更新「資通資產盤點表」，資通資產價值為4者，須會辦資通安全小組；其餘由權責單位主管核定後，呈報資通安全委員會。

5.2 資通資產之報廢

5.2.1 硬體及通訊資產報廢

5.2.1.1 硬體及通訊資通資產需報廢或移作他用，硬體及通訊資產之相關設定與儲存媒體之資料必須清除。

5.2.1.2 硬體及通訊資通資產報廢時，資通資產使用單位應填寫「資通資產異動申請表」，經本校審核並確認資料清除後，方可進行資通資產報廢程序。

5.2.1.3 資通資產保管單位依據「資通資產異動申請表」經本校審核後，辦理更新「資通資產盤點表」，可重複使用之資料儲存媒體，於不再繼續使用時，應將儲存之內容完全消除，敏感級以上的資料必須確認資料清除後無法還原其內容。

5.2.1.4 硬體及通訊資通資產價值為4者，經會辦資通安全小組後，方可執行報廢；資通資產價值為 4 以下者，經權責單位主管核准後，方可執行報廢。

5.2.2 儲存媒體報廢

5.2.2.1 儲存媒體如要報廢或移作他用時，儲存媒體上之資料必須清除。

5.2.2.2 當儲存媒體須報廢時，應採用以下任一種合宜之措施進行銷毀：

5.2.2.2.1 清除硬碟資料

以覆寫方式覆蓋硬碟資料或以工具進行實體之破壞，使其無法使用。

5.2.2.2.2 光碟

於光碟表面塗抹層製造刮痕後，再進行絞碎作業。

5.2.2.2.3 磁帶或磁片

使用強力磁鐵消磁後，磁帶應抽出後剪斷，磁片則進行絞碎作業。

5.2.2.3 儲存機密級以上資料之儲存媒體，嚴格禁止使用格式化方式進行資通資產之報廢程序，應採用上述之方式進行銷毀。

5.2.3 軟體版權到期與移除

5.2.3.1 當軟體版權到期而需移除時，資通資產使用單位應填寫「資通資產異動申請表」，經本校審核後，方可進行軟體移除程序。

5.2.3.2 資通資產保管單位依據「資通資產異動申請表」經本校審核後，辦理更新「資通資產盤點表」。

5.2.3.3 軟體資通資產價值為4者，經會辦資通安全小組後，方可執

行移除；資通資產價值為 4 以下者，經權責單位主管核准後，方可執行移除。

6 相關文件

6.1 資通資產異動申請表

6.2 資通資產盤點表

附件8之附錄1

國立苑裡高級中學-資通資產異動作業					
文件編號	NYLSH-ISMS-01-008	機密等級	限閱	版次	4.0

國立苑裡高級中學資通資產異動申請表

填表日期： 115 年 7 月 15 日

項次	異動別	資產編號	資產類別	資 產 名 稱	權責單位	保管單位	使用單位	資產價值	異 動 說 明
	尚無報廢設備								

使用單位	承辦人		主管		資安長	
資通安全小組	承辦人		主管			

附件9

國立苑裡高級中學-存取控制管理					
文件編號	NYLSH-ISMS-01-009	機密等級	限閱	版次	4.0

1 目的

為保護資通資產，降低未經授權存取系統之風險，以達成國立苑裡高級中學（以下簡稱本校）安全控管之目的。

2 適用範圍

本校資通資產之存取控管原則。

3 權責

本校相關人員、約聘（僱）人員與委外人員遵守相關規定，以確保本校各資通資產之安全。

4 名詞定義

無。

5 作業說明

5.1 存取控制政策

5.1.1 資通資產之存取應與本身業務相關之範圍為主，任何人未經授權不得存取業務範圍外之資通資產。

5.1.2 應正確地使用資通資產，以維護資通資產之可用性、完整性與機密性。

5.1.3 非因業務需求不得將系統存取帳號提供給外部人員，若因業務需要開放帳號予外部人員，應有適當安全控管措施，該安全控管措施應考量業務需求及資通資產之機密性，授與適當之存取權限及有效日期。

5.1.4 被賦予系統管理最高權限之人員、掌理重要技術及作業控制之特定人員，應經審慎之授權評估。

5.1.5 因處理系統當機與異常狀況需視狀況授與適當存取權限，並避免共用帳號。

5.1.6 可攜式電腦儲存媒體，例如：筆記型電腦、隨身碟、外接式硬碟、光碟、磁帶等，應採取適當之控管措施，以防止未經授權之資料、系統、網路存取或病毒傳播。

5.1.7 資料、資訊之存取，必須符合「資通安全管理法」及子法、「個人資料保護法」、「電子簽章法」及「智慧財產權」等相關法規、法令之規定，或契約對資料保護及資料存取使用控管之規定。

5.1.8 系統主機之公用程式路徑之存取權限應適當控管，禁止一般使用者存取。

5.1.9 針對無人看管的資通資產設備，應有適當控管程序，以防未經授權之存取或濫用。

5.1.10 個人桌上型電腦、可攜式電腦應設定於一定時間不使用或離開後，應自動清除螢幕上的資訊並登出或鎖定系統，以避免被未經授權之存取。

5.2 帳號與密碼管理

5.2.1 新購置之應用軟體或系統，安裝完成後應立即更新預設之密碼，並刪除或關閉不必要之帳號。

5.2.2 使用者帳號管理

5.2.2.1 使用者帳號申請應填寫「資訊服務申請表」，經會辦資通安全執行秘書後，由帳號管理人員進行使用者帳號建立作業。

5.2.3 管理者帳號管理

5.2.3.1 系統管理者應避免共用系統管理者帳號，系統管理者帳號與密碼應存放於安全之處。

5.2.3.2 系統管理者密碼設置，至少8碼，且應符合密碼設置原則。

5.2.4 密碼管理

5.2.4.1 使用者首次使用系統時，應要求更改密碼設定，並妥善保管帳號與維持密碼之機密性，保存帳號密碼之檔案應以加密方式處理。

5.2.4.2 使用者應避免將帳號密碼記錄在書面上，張貼在個人電腦、螢幕或其他容易洩漏秘密之場所。

5.2.4.3 使用者禁止共用帳號密碼。

5.2.4.4 使用者發現密碼可能遭破解時，應立即更改密碼。

5.2.4.5 使用者每次存取系統時應輸入密碼登入系統，避免使用記錄密碼功能，導致開機時自動登入系統。

5.2.4.6 資通資產價值為4以上之系統，系統管理者應至少3個月更換密碼一次，學籍系統之使用者(學校行政人員)應至少 6 個月更換密碼一次，並禁止重複使用相同的密碼。

5.2.4.7 使用者密碼設置至少8碼，且應符合密碼設置原則。

5.2.4.8 密碼設置原則

應儘量避免使用易猜測或公開資訊為設定，例如：

A. 個人姓名、出生年月日、身分證字號

B. 機關、單位名稱或其他相關事項

C. 使用者 ID、其他系統 ID

D. 電腦主機名稱、作業系統名稱

E. 電話號碼

F. 空白

密碼設定可考慮下列原則：

A. 參雜數字、英文字母、特殊符號、大小寫

B. 特殊意義詞彙

5.2.4.9 使用者遺忘密碼時，須填具「資訊服務申請表」，經單位主管核准後，由帳號管理人員重新設定。

5.3 使用者存取管理

5.3.1 各項系統資源使用權限之申請、註冊及註銷應遵循作業管理程序，並維護相關之申請、註冊、註銷資料與紀錄，以備查核。

5.3.2 使用者職務異動或離職時，單位主管應即時通知相關單位調整或終止使用者之存取權限。

5.3.3 特殊權限之使用者必須與一般權限之使用者區分管理；針對特殊權限帳號，應妥善管理。

5.3.4 特殊權限之授權管理，必須依執行業務系統別之需求，例如作業

系統、資料庫管理系統、網路服務系統、監控管理系統等賦予系統存取特殊權限的授權，且以執行業務及職務所必要的最低資源存取授權為限。

5.3.5 系統相關作業人員需經正式授權存取業務相關之資通資產，其識別資料與帳號必須為唯一，禁止借用他人之帳號或共用帳號。

5.3.6 各項設備與系統相關之使用權限（例如使用者帳戶與作業權限）應留存紀錄。

5.3.7 應妥善管理久未登錄系統之帳戶，若超過 6 個月未曾登錄，則視需要清除閒置帳號。

5.3.8 應要求使用者變更初始密碼並定期變更密碼；重要資通系統及特殊權限之存取帳號之密碼變更期間應較一般權限之帳號頻繁。

5.3.9 使用者存取權限應定期審查，週期不得超過 6 個月。

5.3.10 重要系統稽核資料應由專人定期審核，系統管理者不得新增、刪除或修改稽核資料，審查週期不得超過 6 個月。

5.3.11 每半年將學籍系統、主機、網路設備等帳號權限設定資料印出，或填寫於「帳號清查紀錄表」，進行帳號權限清查，並將查核結果記錄於「帳號清查結果報告」會辦資通安全執行秘書。

5.4 作業系統存取控制

5.4.1 系統設定應避免於終端機登入程序中以明碼方式顯示密碼相關資訊。

5.4.2 只有在完成所有的登入資料輸入後，系統才開始查驗登入資訊的正確性；若登入發生錯誤，系統不應顯示錯誤發生之原因。

5.4.3 在系統登入被拒絕後，應立即中斷登入程序，並不得給予任何的協助。

5.4.4 應設定系統登入程序之時間限制，如果超出時間限制，系統將自動中斷登入。

5.4.5 使用者帳號避免顯示任何足以辨識使用者特別權限的訊息，例如：顯示其為管理者或監督者。

5.4.6 系統管理人員結束系統維護作業後，應結束應用系統及網路連線，清除螢幕上的資訊，登出系統，並鎖定主控台螢幕。

5.4.7 系統之存取使用應留存查核紀錄。

5.5 應用系統之存取控制

5.5.1 資訊存取之限制

5.5.1.1 應用系統資訊之使用，僅限業務相關之授權使用者，並應適當控制。例如：新增、刪除或執行等。

5.5.1.2 應用系統之敏感與機密性資訊，應與一般資訊作適當區隔，並加強權限控管措施。

5.5.2 原始程式資源之存取控制

5.5.2.1 應用程式原始碼，應集中存放，並由系統負責人管理程式之增修作業。

5.5.2.2 開發中之原始程式碼，應與線上程式碼分開放置與控管。

5.5.2.3 舊版的原始程式應妥慎保管，並詳細記錄使用的明確時間，以備新版失敗回復使用。

5.5.2.4 應用程式之異動需經適當控管。

5.5.2.5 應用程式管理人員，應檢視程式目錄清單，如有異常情形，應即查明原因及處理。

5.6 網路存取控制

5.6.1 網路系統應依其性質之不同，分開成不同的領域，各領域應以特定的安全設施（如防火牆及網路閘門）加以保護，以降低可能的安全風險。

5.6.2 網路管理人員應定期檢視網路存取之紀錄，並留存查核紀錄。

5.6.3 對於開放提供外部客戶或廠商存取之服務，必須限制使用者之網路功能以確保網路安全。

5.6.4 網路路由之規劃必須確保任何網路連線或資訊傳輸符合網路存取之安全需求。

5.7 遠端存取之限制

5.7.1 所有資訊資源使用者，非經單位主管授權或允許，禁止執行遠端存取作業。

5.8 資料庫存取控制

5.8.1 資料庫之存取權限，應經適當程序之授與及移除，且須使用獨立之帳號及密碼登入。

5.8.2 資料庫存取之身分驗證機制，須由系統內部安全機制提供。

5.8.3 資料庫使用者之帳號密碼設定必須符合本程序書及相關系統之帳號密碼管理規範之要求。

5.8.4 資料庫公用程式路徑之存取權限應適當控管，禁止一般使用者存取。

5.8.5 資料庫最高權限帳號之存取授權應僅限於資料庫管理員。

5.8.6 資料庫預設帳號應變更密碼，或是關閉使用。

5.8.7 資料庫之存取紀錄應留存查核紀錄。

5.9 系統被入侵時的異常處理

5.9.1 立即拒絕入侵者任何存取動作（例如關閉可疑帳號），防止災害繼續擴大。

5.9.2 關閉受侵害的主機，或立即與網路離線。

5.9.3 檢查防火牆及系統紀錄，研判入侵管道之方式，必要時作安全漏洞修補。

5.9.4 通知主機供應商提供必要的回復協助。

5.9.5 如伺服主機的完整性受侵害，應將完整的系統備份資料存回受害主機上，並測試其功能，直至完全回復為止，最後再將該主機重新上線。

6 相關文件

6.1 資訊服務申請表

6.2 帳號清查紀錄表

6.3 帳號清查結果報告

附件9之附錄1

國立苑裡高級中學-存取控制管理					
文件編號	NYLSH-ISMS-01-009	機密等級	限閱	版次	4.0

國立苑裡高級中學資訊服務申請表

填表日期：　　年　　月　　日

申請人簽章	
申請項目： □申請學校首頁帳號 □申請電子郵件帳號　　□申請密碼重置： □申請校務行政系統帳號(未特別要求，帳號將與學校 Google 帳號@前相同) □申請校內 NAS 帳號(原因說明請勾選其他並註明學校 Google 帳號) □其它：_____	
原因說明： □新進教職員工(□正式人員　□代理教師或約聘顧人員) □職務異動 □忘記密碼 □其他：_____ (以上由申請人填寫)	
審核結果：□同意　□不同意	
審核意見說明：	
承辦人：	主管：
完成日期：_____年____月____日	

附件9之附錄2

國立苑裡高級中學-存取控制管理					
文件編號	NYLSH-ISMS-01-009	機密等級	限閱	版次	4.0

國立苑裡高級中學帳號清查紀錄表

填表日期：115年 6 月15 日

項次	系統名稱	帳號	使用者	權限說明	備　註
1	學校官網	ylshmlc02	吳政璟	網站管理員	
2	學校官網	ylshmlc004	郭勝宗	編輯	
3	學校官網	ylshmlc005	陳建宇	編輯	
4	學校官網	ylshmlc006	李宗儒	編輯	
5	學校官網	ylshmlc007	陳芯雩	編輯	
6	學校官網	ylshmlc008	鄭湘怡	編輯	
7	學校官網	ylshmlc009	卓靖雪	編輯	
8	學校官網	ylshmlc010	涂瑞儀	編輯	
9	學校官網	ylshmlc011	鄭孟淳	編輯	
10	學校官網	ylshmlc012	林芊蕙	編輯	
11	學校官網	ylshmlc014	李名媛	編輯	
12	學校官網	ylshmlc017	羅巧芳	編輯	
13	學校官網	ylshmlc019	陳秀香	編輯	
14	學校官網	ylshmlc020	劉淑娟	編輯	

15	學校官網	ylshmlc021	鄭燕琪	編輯	
16	學校官網	ylshmlc023	錢尹鑫	編輯	
17	學校官網	ylshmlc025	洪玉靜	編輯	
18	學校官網	ylshmlc027	羅佳勝	編輯	
19	學校官網	ylshmlc028	朱家賢	編輯	
20	學校官網	ylshmlc029	曾淑華	編輯	
21	學校官網	ylshmlc030	吳淑貞	編輯	
22	學校官網	ylshmlc037	周文雅	編輯	
23	學校官網	ylshmlc039	林佳慧	編輯	
24	學校官網	ylshmlc040	黃彩鑾	編輯	
25	學校官網	ylshmlc045	鍾木根	編輯	
26	學校官網	ylshmlc046	張憶梅	編輯	
27	學校官網	ylshmlc050	張明智	網站管理員	

附件9之附錄3

國立苑裡高級中學-存取控制管理					
文件編號	NYLSH-ISMS-01-009	機密等級	限閱	版次	4.0

國立苑裡高級中學帳號清查結果報告

填表日期： 115 年 6 月 17 日

承辦單位	資媒組	清查日期	**115.06.17**
清查項目	□____系統 ■學校首頁 □電子郵件帳號 □校內ＮＡＳ □資料庫（_____） □其它_____		
備　註			

清　查　結　果			
清查前帳號總數	27	清查後帳號總數	27
本次註銷帳號數	0	本次權限變更帳號數	0

細　項　說　明				
帳　號	使用單位	使 用 人	異　動　方　式	異動原因說明
無			□新增 □註銷 □調整權限 □其它_____	
			□新增 □註銷 □調整權限 □其它_____	
			□新增 □註銷 □調整權限 □其它_____	
			□新增 □註銷 □調整權限 □其它_____	

業務單位 承辦人及主管簽章	資通安全小組 承辦人及主管簽章

附件10

國立苑裡高級中學-實體安全管理					
文件編號	NYLSH-ISMS-01-010	機密等級	限閱	版次	4.0

1 目的

為保護國立苑裡高級中學（以下簡稱本校）資通資產及周邊環境設施，減少環境安全問題所引發的危險，以便達成本校安全控管之目的。

2 適用範圍

本校機房及周邊環境與設備安全管理。

3 權責

本校相關人員、約聘（僱）人員與委外人員遵守相關規定，以確保本校安全區域與人員辦公區域及資通資產設備之安全。

4 名詞定義

無。

5 作業說明

5.1 安全區域

5.1.1 本校之機房為安全區域。

5.1.2 為確保相關設施之安全，非權責單位授權之人員不得擅自進入安全區域或使用相關資通設備。

5.1.3 若外部人員或本校未具機房進出權限之人員，因執行業務需求進入機房時，必須由資通資產權責單位或保管單位指派人員隨行並填寫「人員進出機房登記表」後方可進出機房，並遵守相關設備管理之規定。

5.1.4 安全區域之門禁紀錄，該紀錄應適當保存與定期審閱。

5.2 一般控制措施

5.2.1 無人時或下班最後一人離開時，需將辦公室關門上鎖。

5.2.2 為防止未經授權之存取，同仁應於下班後，遵守桌面淨空政策，並將敏感等級（含）以上之文件與可攜式資通設備皆存放於儲櫃並上鎖，避免資訊外洩之機會。

5.2.3 同仁於本校安全區域與辦公室內需隨時注意身分不明或可疑的人員。發現不明身分之人員時，需主動詢問並儘速通知相關部門進行處理。

5.2.4 同仁需隨時清理個人電腦的資源回收筒，以確保已經刪除的重要資料不會因為遺留在資源回收筒未清理，而遭未經授權之使用。

5.2.5 未經授權不得將設備、軟體、儲存資訊之媒體或文件攜出安全區域。如有需要，則須經權責單位主管核准，始得進行。

5.3 一般設備安全

5.3.1 資通資產與相關設備安全之維護需考量設備之使用、安置、儲存、監控、移出與報廢等安全管理。

5.3.2 可攜式電腦，需以密碼保護，免於被偷取、遺失而遭未經授權的盜用，並於使用完畢後，刪除電腦中非一般等級之資料及清理資源回收筒內之資料。

5.3.3 個人電腦、伺服器或電腦終端機不使用時，需採用密碼保護、鎖定或登出離線等安全控制措施。

5.4 硬體資通資產安全維護

5.4.1 重要之儲存媒體，應上鎖或由專人管理，並且僅經授權之使用者方能使用。

5.4.2 謹慎使用電源延長線，以免電力無法負荷而導致火災，於新增硬體設備時，應先評估電力負荷。

5.4.3 設備異動（包含新增、報廢、變更用途），應重新評估相關系統設定。

5.5 機房設備安全維護

5.5.1 重要資通設備，應放置於機房，並落實安全管理。

5.5.2 電力、網路、通信設備應予以保護，以防止遭有心人士截取或破壞。

5.5.3 機房內應保持整齊清潔，並嚴禁吸菸、飲食或堆置易燃物。

5.5.4 電腦機房應設置專用空調設備以維持電腦主機正常運作。

5.5.5 經評估後，確定將資通設備（如：伺服器、防火牆…等）委外維護時，應簽訂維護契約，並定期實施保養與維護，以確保設備完整性及可用性之持續使用。

5.5.6 重要電腦主機之資通設備及警報系統等應定期檢修測試。

5.5.7 冷氣機、不斷電系統（UPS）等機電設備之使用，應依照設備說明書指示操作，並施行定期檢查作業。

5.5.8 機房應設置足量之不斷電系統（UPS），供應重要資通設備電源之使用，以保障資通設備之正常作業。

5.5.9 機房溫溼度應維持在機器可正常運轉的範圍內，並需 24 小時維持空調運轉。

5.5.10 資通設備專用電源插座，不得使用於資通及空調設備以外之設備，以免耗用電源，發生跳電當機情形，影響正常作業。

5.5.11 資通設備保管單位應於每工作日檢核各設備之運作狀況，發現異常時，應填寫「異常事件紀錄表」並進行必要之處置。

5.6 移轉資產之安全管理

5.6.1 機房中資通設備之進出應填寫「設備進出紀錄表」敘明其設備進出原因或目的。

5.6.2 資通設備、資料或軟體之移轉，應依據「資通資產異動作業」辦理，並由資通安全小組負責更新「資通資產盤點表」。

5.6.3 硬體資產報廢前應確實清除限閱等級（含）以上之資訊，以避免資訊外露，並確實清點報廢資產後，方可進行報廢。

5.7 送修作業

5.7.1 資通設備送修前，資通設備之權責單位應依該設備之資通資產價值選擇適當之備援方案，並備註說明於「設備進出紀錄表」。

5.7.2 資通設備若具敏感等級以上之資料，於送修前應請廠商簽署「委外廠商執行人員保密切結書」。

5.8 維護契約

5.8.1 所有資通設備維護契約，應由專人負責保管與定期審查契約時間是否過期與該資通設備是否仍有維護需求。

6 相關文件

6.1 資通資產管理

6.2 資通資產異動作業

6.3 資通資產盤點表

6.4 人員進出機房登記表

6.5 異常事件紀錄表

6.6 設備進出紀錄表

6.7 委外廠商執行人員保密切結書

附件10之附錄1

國立苑裡高級中學-實體安全管理					
文件編號	NYLSH-ISMS-01-010	機密等級	限閱	版次	4.0

國立苑裡高級中學人員進出機房登記表

填表日期：　年　月　日

年　月　日	進入時間		進入單位人員	
	離開時間		校內陪同人員	
事由：□設備維護 (□資通 □電力 □空調 □消防 □其他_____) □保全系統維護 攜出入物品簡述：(簡述物品名稱，細節請另填設備進出登記表)				

附件10之附錄2

國立苑裡高級中學-實體安全管理					
文件編號	NYLSH-ISMS-01-010	機密等級	限閱	版次	4.0

異常事件紀錄表

填表日期：　年　月　日

異常原因	異常發現時間：　　年　　月　　日　　時　　分	
處理說明	異常排除時間：　　年　　月　　日　　時　　分	
承辦人		主管

附件10之附錄3

國立苑裡高級中學-實體安全管理					
文件編號	NYLSH-ISMS-01-010	機密等級	限閱	版次	4.0

國立苑裡高級中學設備進出紀錄表

填表日期：　年　月　日

□攜入 □攜出	時間		攜　出(入) 單　位	
設備名稱			財產編號	
設備序號 品牌/規格				
攜進/出方式	□自行攜進/出 □貨運代送（公司名稱/電話：_____ 貨運編號：_____） □其他（請說明：_____）			
攜進/出原因	□新增設備 □設備送修（預計完成日期：　/　/　） □安裝設定（預計完成日期：　/　/　） □調 / □借 / □還 單　位：_____ 聯 絡 人：_____ 聯絡電話：_____ （預計歸還日期：　/　/　） □其他（請說明：_____）			
覆核單位				
承辦人		主管		

附件11

國立苑裡高級中學-通信與作業管理					
文件編號	NYLSH-ISMS-01-011	機密等級	限閱	版次	4.0

1 目的

為防止國立苑裡高級中學（以下簡稱本校）資訊在不安全之網路環境下，遭致可能之破壞，或非預期及非經授權之修改，以確保資通系統與資料之安全性、可用性及完整性。

2 適用範圍

本校所轄之範圍內，相關網路服務與設備及核心資通系統之管理。

3 權責

本校網路管理人員應遵守本程序書之相關規定，以確保本校網路之安全。

4 名詞定義

4.1 機密性(Confidentiality)：確保只有經授權的人，才可以存取資訊。

4.2 完整性 (Integrity)：確保資訊與處理方法的正確性與完整性。

4.3 可用性 (Availability)：確保經授權的使用者在需要時可以取得資訊及相關資產。

4.4 可接受風險值：各類資通資產之最低風險容忍度。

4.5 殘餘風險 (Residual Risk)：在採用相關控制措施之後剩餘的風險。

4.6 威脅 (Threat)：可能對系統或組織造成傷害之意外事件。

4.7 弱點(Vulnerability)：因資通資產本身狀況或所處環境之下，可能受到威脅利用而造成資產受到損害之因子。

4.8 風險 (Risk)：可能對團體或組織的資產發生損失或傷害的潛在威脅，通常利用弱點所產生之影響及發生可能性來衡量。

4.9 行動計算與通信設施：如筆記型電腦、掌上型電腦、行動電話等。

4.10儲存媒體：如磁片、磁碟、磁帶、IC 卡、匣式磁帶、外接式硬碟、光碟、隨身碟、各式記憶卡、錄影帶、錄音帶等。

5 作業說明

5.1 資通系統安全規劃作業

5.1.1 應建立資通系統之安全控管機制，以確保資訊資料之安全，保護系統及網路作業，防止未經授權之系統存取。

5.1.2 資通系統管理職務與責任應加以區隔，足以影響業務經營管理的資訊，不可只由單獨一人知悉。如因人力資源限制，無法區隔責任，則應加強監督與稽核等措施。

5.1.3 伺服主機及網路設備應指定負責人，負責該主機之正常運作，包括應用程式之執行、資料庫之維護及相關作業系統與主機硬體資源之分配管理。主機或網路設備負責人無法進行管理時應由代理人負責，未指定負責人之主機及網路設備由機房管理負責人員負責。

5.1.4 網路管理人員應妥為規劃網路架構、設定網路參數，並依規定備份相關檔案。

5.1.5 應規劃系統與設備的開發與測試環境，避免於已上線運作設備及環境進行開發或測試工作。

5.1.6 系統及設備建置前，主辦單位應對系統需求做適當規劃，以確保足夠的電腦處理及儲存容量。

5.1.7 系統設備與軟體之建置，均應依據「系統開發與維護」進行測試及驗收。

5.2 變更管理

5.2.1 新增設備及網路變動，應即時修改網路架構圖及設備資料。

5.2.2 架構調整：架構變動之影響性甚大者應會辦資通安全小組，並遵循下列規定：

5.2.2.1 設備之功能性及設定方式應熟悉掌握。

5.2.2.2 新增對外網路連線，需注意安全性考量，從嚴審核對外網路連線與內部之連接之方式。

5.2.2.3 如有廠商參與安裝或設定，必須全程陪同參與並記錄。

5.2.3 系統若有相關文件（如系統文件、參考文件或作業準則）時，系統相關負責人員於變更程序同時，應同步修改維護相關文件。

5.2.4 各項系統變更作業依據「系統開發與維護」變更作業控制措施辦理。

5.3 惡意軟體之防範

5.3.1 禁止使用或下載未經授權或與業務無關之軟體。

5.3.2 應安裝病毒偵測與修復軟體，並定期更新病毒資訊，以防止病毒之攻擊。伺服器主機防毒軟體系統應設定主動掃瞄檢查，或由網路管理人員定期執行掃瞄檢查作業。

5.3.3 應定期檢查支援重要業務之作業系統是否有任何未核准的檔案或未經授權的修改。

5.3.4 應於使用來源不明、來源未經授權、或從未經信任網路接收之檔案前，檢查該檔案是否藏有病毒。

5.3.5 應於使用前檢查電子郵件附件和下載檔案有無惡意軟體。

5.3.6 使用者如偵測到電腦病毒入侵或其他惡意軟體，應立即通知系統或網路管理人員；管理者亦應將已遭病毒感染的資料及程式等資訊隨時提供使用者，以避免電腦病毒擴散。

5.3.7 系統或電腦設備如遭病毒入侵感染，應立即與網路離線並隔離，直到網路管理人員確認病毒已消除後，才可重新連線，並留存處理紀錄。

5.4 電腦軟體與程式著作權保護

5.4.1 應訂定使用授權軟體與遵守著作權規範，違反規範者應依相關程序議處。

5.4.1.1 使用軟體與資通產品不得超過允許的最高使用人數。

5.4.1.2 使用軟體與資通產品應遵守相關規定，例如限制於指定之機器使用、限制僅於備份時方可複製等。

5.4.1.3 取得之合法軟體不得從事或轉讓予非授權範圍之使用。

5.4.1.4 從公共網路取得之合法軟體與資訊須遵守原著作權者與電腦處理個人資料保護法之規定。

5.4.1.5 對公共系統的存取不得擅自存取其所相連的網路。

5.4.2 應妥善保管採購軟體產品之授權書、原版光碟、手冊等等證明。

5.4.3 經由網際網路下載之公開授權軟體，應在確認安全無虞及不違反智慧財產權前提下，方得下載執行。

5.5 網路安全管理

5.5.1 網路服務之管理

5.5.1.1 避免利用公共網路傳送敏感等級（含）以上資訊，應保護資料在公共網路傳輸之完整性及機密性，並保護連線作業系統之安全性。

5.5.1.2 網路管理人員應利用網路管理工具，偵測及分析網路流量。

5.5.1.3 開放相關人員從遠端登入內部網路系統之網路服務，應執行嚴謹之身分辨識作業，或提供連線設備之識別機制。

5.5.1.4 如果系統使用者為非合法授權之使用者時，應立即撤銷其系統使用權限；離（休、退）職人員應依據資通安全規定及程序，調整或終止其存取網路及系統之權限。

5.5.1.5 網路管理人員除依據相關法令或規定，不得閱覽使用者之私人檔案；但如發現有可疑之網路安全情事，網路系統管理人員得依授權規定，使用工具檢查檔案。

5.5.1.6 網路管理人員除有緊急狀況外，未經使用者同意，不得增加、刪除及修改私人檔案。

5.5.1.7 網路設備軟硬體應限定由網路系統管理人員依據規定辦理設定異動，並應留存紀錄備查。

5.5.1.8 網路管理人員應於每工作日檢查所有網路設備並記錄於「巡查紀錄表」，每月送單位主管簽核。如發現異常應依據本程序之異常處理流程辦理。

5.5.2 網路使用者之管理

5.5.2.1 經授權之網路使用者，只能在授權範圍內存取網路資源。

5.5.2.2 網路使用者於使用行動碼（如 ActiveX、JAVA Applet）之前，應先確認其授權資料，並禁止執行未經授權之行動碼。

5.5.2.3 網路使用者應遵守網路安全規定，並確實瞭解其應負之責任；如有違反網路安全情事，應依據資通安全規定，限制或撤銷其網路資源存取權利，並依據相關規定處理。

5.5.2.4 網路使用者不得將自己之登入身分識別與登入網路之密碼交付他人使用。

5.5.2.5 禁止網路使用者以任何方法竊取他人之登入身分與登入網路密碼。

5.5.2.6 禁止網路使用者以任何儀器設備或軟體工具竊聽網路上之通訊。

5.5.2.7 禁止網路使用者在網路上取用未經授權之檔案。

5.5.2.8 網路使用者不得將色情檔案建置在網路，亦不得在網路上散播色情文字、圖片、影像、聲音等不法或不當之資訊。

5.5.2.9 禁止網路使用者發送電子郵件騷擾他人，導致其他使用者之不安與不便；或以任何手段蓄意干擾或妨害網路系統之正常運作。

5.5.2.10網路使用者不得任意修改網路相關參數。

5.5.3 無線網路使用之管理

5.5.3.1 無線網路基地台之使用應經適當控管。

5.5.3.2 無線網路設備之安裝設定應經核准。

5.5.3.3 無線網路設備之使用應取得授權，禁止於內部網路私自使用任何無線網路產品。

5.5.3.4 無線網路設備之使用應有適當管理機制，例如：授權使用之 IP 數量、連接埠、網卡位址（MAC）過濾等。

5.5.3.5 無線網路之資料傳輸應使用加密機制，並就安全與資訊風險之考量，增加適當之防護機制以避免資料外洩。

5.5.4 防火牆之安全管理

5.5.4.1 所有與外界網路連接之連線，應透過加裝防火牆，以控管外界與本校內部網路間之資料傳輸與資源存取。

5.5.4.2 防火牆設定異動時，應填寫「防火牆進出規則申請表」，經單位主管簽准後，交由網路管理人員設定。

5.5.4.3 防火牆應由網路管理人員執行控管設定，並依制定之資通安全規定、資通安全等級及資源存取之控管策略，建立包含身

分辨識機制與系統稽核之安全機制。

5.5.4.4 防火牆設置完成時，應測試防火牆是否依設定之功能正常及安全地運作。如有缺失，應立即調整系統設定，直到符合既定之安全目標。

5.5.4.5 網路管理人員應配合資通安全政策及規定之修正，以及網路設備之變動，隨時檢討及調整防火牆系統設定，調整系統存取權限，以反映最新狀況。

5.5.4.6 視業務需要及設備功能，對於通過防火牆之特定網路服務，應予確實紀錄。

5.5.4.7 網路管理人員應避免採取遠端登入方式登入防火牆主機，以避免登入資料遭竊取，危害網路安全。如果必須使用遠端登入方式管理，應訂定嚴謹之遠端登入控管措施。

5.5.4.8 若資源許可應建立防火牆設備之備援機制；防火牆之環境建置檔等需定期執行備份作業。

5.5.4.9 防火牆政策及設定應每月定期覆核，並記錄於「巡查紀錄表」中，若已屆期限或該IP不再使用，請系統負責人確認後刪除，並填寫「防火牆進出規則申請表」。

5.5.4.10網路管理人員每週將防火牆之log轉出存放於備份機器上，並記錄於「巡查紀錄表」。

5.5.4.11於防火牆設定變更之前，將各防火牆之設定檔備份，並依「備份狀況紀錄表」之表列進行備份，存放於備份設備上。

5.5.5 網路資訊之管理

5.5.5.1 敏感等級（含）以上之業務資料或文件不得存放於對外開放之資通系統中，若因特殊業務功能之需求，必須採取加強之安全管控機制，如：資料加密。

5.5.5.2 網路管理人員應負責監督網路流量及使用情形，並對可能導致系統作業癱瘓等情事，預作有效的防範，以免影響網路服務品質。

5.5.5.3 對外開放的資通系統所提供之網路服務，如：HTTP、FTP 等，應採取適當之存取控管機制。

5.5.5.4 對校外開放的資通系統，如：存放教職員、學生或家長申請或註冊之個人資料檔案，其傳輸過程應考量以加密方式處理，並妥善保管資料，以防止被竊取或移作他途之用，侵犯個人隱私。

5.5.5.5 網路管理人員於偵測收到資通系統異常狀況或駭客入侵之警示訊息時，應立即通報單位主管，依據相關作業管理規範採取適當之緊急應變處理，並留存系統異常處理紀錄。

5.5.6 網路管理作業流程

5.5.6.1 網路檢查作業

5.5.6.1.1 以指令方式 ping 各網段之 Gateway，以回應時間初步判斷網路狀態。

5.5.6.1.2 檢查防火牆之 log 及狀態。

5.5.6.1.3 防火牆發現異常情形應設定自動寄發通知信給網路管理人員，嚴重時網路管理人員應立即採取阻擋作為，並通知單位主管。

5.5.6.2 網路監控作業

5.5.6.2.1 利用工具自動 ping 各 IP，用以監控網路各節點，由其回應數值判斷網路狀態是否正常。

5.5.6.2.2 收集防火牆之 log，並統計 log 資料。

5.5.6.2.3 監控內部網路頻寬使用狀況，於頻寬使用率達 60%以上時，應評估增加頻寬之必要性。

5.5.6.3 異常監控作業

5.5.6.3.1 定期監控各伺服器提供之各項服務是否正常，若設備服務狀態不正常時，應通知相關負責人員處理。

5.5.6.4 異常處理作業

5.5.6.4.1 以節點方式由內而外檢測，由回應數值推知問題點。

5.5.6.4.2 確認與問題點相關之實體設備和網路線是否正常。

5.5.6.4.3 如為設備問題可尋找替用設備更換，並連絡廠商維修，並將處理情形記錄於「異常事件紀錄表」。

5.5.7 網路入侵之處理

5.5.7.1 應建立網路入侵事件之調查程序，除利用工具及稽核檔案提供之資料外，應協請相關單位（如網路服務提供者），追蹤入侵者。

5.5.7.2 入侵者之行為若觸犯法律規定，構成犯罪事實，應立即告知相關單位，請其處理入侵者之犯罪事實調查。

5.6 電子郵件安全管理

5.6.1 電子信箱帳號之註冊、離職、異動申請，應遵循電子郵件相關管理規範之規定，除學生帳號由本校批次建立外，其餘則填寫「資訊服務申請表」提出申請，經單位主管核准後，再交由系統管理者或經授權之管理者建置相關資料。

5.6.2 應建立電子郵件之安全管理機制，以降低電子郵件可能帶來之業務上及安全上之風險。

5.6.3 應禁止發送匿名信，或偽造他人名義發送電子郵件騷擾他人，導致其他使用者之不安與不便。

5.6.4 敏感等級（含）以上的資料或文件，應避免以電子郵件傳送。

5.6.5 不得傳遞大量且非必要的資訊，避免網路壅塞及資源浪費。

5.6.6 電子郵件附加之檔案，應事前檢視內容有無錯誤後方可傳送。

5.6.7 對來路不明之電子郵件，不宜隨意打開電子郵件，以免啟動惡意執行檔，使網路系統遭到破壞。

5.6.8 郵件伺服器異常處理及故障排除作業

5.6.8.1 發現郵件伺服器系統異常，資訊人員應進行診斷，辨識異常原因及影響範圍，評估系統回復時間，並進行排除作業。

5.6.8.2 異常處理人員應定時回報單位主管最新狀況及處理進度。

5.6.8.3 如異常發生無法立即排除故障時，應通知相關部門異常影響程度及預估回復時間，並採取因應措施。

5.6.8.4 如診斷可能係硬體設備故障造成，則通知廠商人員到場檢測。

5.6.8.5 系統經復原並確實檢查測試後，終止緊急應變作業，並通

知相關部門及其主管。

5.6.8.6 將處理過程及結果記錄於「異常事件紀錄表」中。

5.7 全球資訊網（WWW）

5.7.1 對 HTTP 伺服器開放可存取的範圍，應限制僅能存取資訊系統之某一特定區域之功能與權限，HTTP 伺服器應透過組態的設定，使其啟動時不具備系統管理者身分。

5.7.2 公告之資訊，應經由權責管理人員之審查與核定，確認未含機密性或敏感性的資訊、違反本系統資通安全管理之相關資訊，以及違反智慧財產權或法令所明定禁止之資訊。

5.7.3 開放外界連線作業之資通系統，應避免外界直接進入資通系統或資料庫存取資料。

5.7.4 內部使用的瀏覽器，對下載之檔案應設定掃描是否隱藏電腦病毒或惡意內容。

5.7.5 當伺服器執行之應用程式需接收自使用者回傳資料時，應予嚴密監控，以防止不法者利用來執行系統指令，獲取系統內重要的資訊或破壞系統。

5.8 電腦管理及安全防護

5.8.1 系統負責人應定時檢查作業系統及硬體設備之效能，並注意作業系統版本更新及問題資訊，做最適建議及導入。

5.8.2 主機負責人應進行伺服器主機監控，檢查系統、安全及應用程式日誌紀錄、或其它有關之系統狀況。一旦發現任何問題得請相關人員協同處理，必要時並通知廠商處理。

5.8.3 為提升伺服器主機連線作業之安全性，應視需要使用加密通道（如 VPN、SSH）等各種安全控管技術。

5.8.4 應關閉不需要之服務。

5.8.5 系統負責人需定期檢視更新系統安全修補、防毒軟體及防毒碼，以維持系統正常運作。

5.8.6 應保存稽核紀錄，並定期審查。

5.8.7 系統負責人應於每工作日上班時依據「巡查紀錄表」所列項目檢

查各主機狀況，以確保系統正常運作。

5.8.8 軟體由系統負責人安裝，安裝時應視狀況通知相關技術人員支援或通知使用者，以避免資訊服務中斷或影響業務。

5.8.9 系統軟體測試由系統負責人辦理，測試時應事先公告並通知及協調相關人員支援，且視狀況需要通知相關人員及使用者以避免因資訊服務中斷而影響業務。

5.8.10 異常狀況排除

5.8.10.1遇異常狀況時系統負責人應先行回報資通安全小組，視需要採適當方式處理。

5.8.10.2通知本校相關人員協助，並說明詳細原因、先行處理步驟及相關資料。如無法自行排除則向維護廠商報修維護，並將故障情形公告及通知使用者及相關人員。

5.8.10.3將處理過程及結果記錄於「異常事件紀錄表」中。

5.8.11 系統入侵之處理

5.8.11.1立即拒絕入侵者任何存取動作（例如關閉可疑帳號），以防止災害繼續擴大。

5.8.11.2關閉受侵害的主機，並立即與網路離線。

5.8.11.3檢查防火牆及系統紀錄，研判入侵管道之方式，必要時作安全漏洞修補。

5.8.11.4通知主機供應商提供必要的回復協助。

5.8.11.5如伺服主機的完整性受侵害，應將完整的系統備份資料存回受害主機上，並測試其功能，直至完全回復止，最後再將該主機重新上線。

5.8.11.6將處理過程及結果記錄於「異常事件紀錄表」中。

5.9 可攜式電腦儲存媒體管理

5.9.1 系統資料若需以可攜式媒體保存時，該媒體應存放於安全設備或處所。

5.9.2 儲存媒體所使用之密碼或編碼技術不應透露予遞送人員或與業務無關之人員。

5.9.3 儲存媒體遞送前應加以妥善包裝保護，避免發生實體損壞。

5.9.4 儲存媒體如委由外部單位（例如：郵局或快遞公司）運送，應選擇具有信譽之廠商，並採取以下控制措施：

5.9.4.1 放置於上鎖之容器或以彌封方式處理。

5.9.4.2 當面送達並簽收。

5.9.4.3 資料內容應使用密碼保護。

5.9.5 該儲存媒體之報廢，請詳「資通資產異動作業」，且須經核准。

5.10資料備份

5.10.1 各項系統設定檔、伺服器檔案及資料庫資料均應由各系統負責人員訂定備份週期，並依據週期執行系統排程或手動備份，備份狀況應記錄於「備份狀況紀錄表」。

5.10.2 應定期於測試主機上測試備份復原是否正確。

5.10.3 重要系統資料應考量建立異地備份機制。

5.11安全稽核事項

5.11.1 對各項系統視需要留存系統最新參數設定檔。

5.11.2 系統管理、技術諮詢與機房操作人員工作應依職務與相關規定確實記錄其工作內容於「巡查紀錄表」內。

5.11.3 每月應檢視一次各設備中系統時間是否一致，並進行校正及同步作業。

5.11.4 系統稽核資料應依系統重要性進行備份保護作業，並由專人定期審核，系統管理者不得新增、刪除或修改稽核資料，審查週期不得超過6個月。

5.11.5 應定期查核技術符合性，進行弱點掃描或滲透測試，以確定資通系統及網路環境符合安全實施標準。掃描週期如下：

5.11.5.1每半年至少針對伺服器及網管設備執行一次。

5.11.5.2當系統有重大變動時。

5.11.5.3新系統上線前。

5.11.6 系統異常及安全事件記錄與分析，依據「矯正及預防管理程序書」辦理。

5.11.7 弱點掃瞄報告與修補作業

5.11.7.1執行弱點掃描應產出弱點掃描報告，弱點掃描報告格式不拘，惟應包含下列內容：

5.11.7.1.1弱點掃描檢測範圍。

5.11.7.1.2弱點掃描檢測時程。

5.11.7.1.3弱點風險等級說明。

5.11.7.1.4安全弱點列表與建議修補措施。

5.11.7.2掃描出之弱點應限期改善，並填寫「弱點處理報告單」，且於修補後進行複掃。

5.11.7.3於安裝修正程式前，需先行測試並確認運作正常後，方可進行安裝。

5.11.8 殘餘弱點管理

5.11.8.1弱點若因故無法修補，應於「弱點處理報告單」說明無法修補之原因與防禦因應方法。

6 相關文件

6.1 資通安全政策

6.2 系統開發與維護

6.3 資通資產異動作業

6.4 巡查紀錄表

6.1 防火牆進出規則申請表

6.2 備份狀況紀錄表

6.3 實體安全管理

6.4 異常事件紀錄表

6.5 弱點處理報告單

附件11之附錄1

國立苑裡高級中學-通信與作業管理					
文件編號	NYLSH-ISMS-01-011	機密等級	限閱	版次	4.0

國立苑裡高級中學巡查紀錄表

日期 \ 檢查項目				伺服主機狀態	設備燈號	網路狀況	溫度(℃)	溼度(%)	防火牆政策及設定(每月第一個工作天) 其他事件說明	簽章
年 月	週次	日期	星期							
	第一週		一						每月第一個工作天： □主防火牆設定備份 □主防火牆政策檢核 □Wifi控管設定備份 □Wifi控管設定檢核 □電教控管設定備份 □電教控管設定檢核 其他事件說明： □無(每月最後一天) □有，說明如下。	
			二							
			三							
			四							
			五							
	第二週		一							
			二							
			三							
			四							
			五							
	第三週		一							
			二							
			三							
			四							
			五							
	第四週		一							
			二							
			三							
			四							
			五							
	第五週		一							
			二							
			三							
			四							
			五							

國立苑裡高級中學-通信與作業管理					
文件編號	NYLSH-ISMS-01-011	機密等級	限閱	版次	4.0

國立苑裡高級中學防火牆進出規則申請表

<table>
<tr><td>*申 請 人</td><td colspan="2"></td><td>*申請日期</td><td></td></tr>
<tr><td>*申請說明</td><td colspan="4"></td></tr>
<tr><td rowspan="2">*防火牆授權</td><td>有效
時間</td><td>起：
迄：</td><td>Port</td><td></td></tr>
<tr><td>來源 IP</td><td></td><td>目的 IP</td><td></td></tr>
<tr><td>應用程式</td><td colspan="4">□(請在填寫來源 IP)
□(請在填寫上方 Port、來源 IP 與目的 IP)
□其他：_____</td></tr>
<tr><td rowspan="2">處理記錄</td><td>NAT</td><td colspan="3">□是 □否</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="2">規則編號 #</td><td colspan="3"></td></tr>
<tr><td colspan="2">設定檔備份 □是</td><td colspan="3">Firewall Check □是</td></tr>
<tr><td>承辦人</td><td></td><td>主管</td><td colspan="2"></td></tr>
</table>

附件11之附錄3

國立苑裡高級中學-通信與作業管理					
文件編號	NYLSH-ISMS-01-011	機密等級	限閱	版次	4.0

國立苑裡高級中學備份狀況紀錄表

填表日期：115 年 7 月 15 日

備份周期	備份項目（伺服器/資料庫/網站/其他）	儲存媒體/IP/可用空間紀錄	檢查人員簽章	備註
每週	所有虛擬機	NAS/172.17.0.201/39.6T		

主管：_____

附件11之附錄4

國立苑裡高級中學-通信與作業管理					
文件編號	NYLSH-ISMS-01-011	機密等級	限閱	版次	4.0

國立苑裡高級中學弱點處理報告單

填表日期： 年 月 日

設備名稱		系統名稱		管理人員	
外部 IP		內部 IP		掃瞄時間	年 月 日

項次	等級	弱點名稱	修補情形	修補日期	未修補原因說明與防禦因應方法
			□已修補 □暫不修補		
			□已修補 □暫不修補		
			□已修補 □暫不修補		
			□已修補 □暫不修補		
承辦人			主管		

附件12

國立苑裡高級中學-系統開發與維護					
文件編號	NYLSH-ISMS-01-012	機密等級	限閱	版次	4.0

1 目的

為確保國立苑裡高級中學（以下簡稱本校）資通系統開發、測試與維護作業之安全管理。

2 適用範圍

資通系統之程式開發相關支援活動，如既有線上系統之測試、修改、維護、上線變更、原始碼之管控與儲存等作業。

3 權責

本校相關資通系統開發、維護人員與委外人員遵守相關規定，以確保本校相關軟體與資料等資通資產之安全。

4 名詞定義

無。

5 作業說明

5.1 一般控制措施

5.1.1 當發展新資通系統，或現有系統功能之強化，於系統規劃需求分析階段，即將安全需求要項納入系統功能。

5.1.2 除由系統自動執行之安全控管措施之外，亦可考量由人工執行相關控管措施。

5.1.3 在採購套裝軟體時，視其安全需求，進行分析。除事前經權責單位主管核准外，應避免修改套裝軟體，如需修改應依本程序書之變更作業控制措施加以控管。

5.1.4 系統之安全需求及控制程度，應與資通資產價值相稱，並考量安全措施不足，可能帶來之傷害程度。

5.1.5 資通系統應保護敏感等級（含）以上之資料，防止洩漏或被竄改，必要時應使用資料加密之相關機制保護。

5.1.6 在作業系統上執行應用軟體，應建立控制程序並嚴格執行，為減少可能危害作業系統之風險，應用程式之更新作業應限定只能由授權之管理人員才可執行，且應建立應用程式之更新稽核紀錄。

5.1.7 真實資料被複製到測試系統時，應依複製作業之性質及內容，在取得授權後始能進行，敏感資料欄位應予模糊化。

5.1.8 系統若需委外建置或維護，請參考資通安全維護計畫壹拾貳、資通系統或服務委外辦理之管理、政府資訊服務採購作業指引、依「資通安全責任等級分級辦法」執行系統防護需求等級之相關防護控制措施（附表九、資通系統防護需求分級原則及附表十、資通系統防護基準），並符合資通安全管理法及子法、個人資料保護法及施行細則等法遵。

5.1.9 系統弱點管理，請參考「通信與作業管理」之相關管理規範。

5.1.10 各單位若有資料需求申請時，申請人視情況應依電子公文程序或填寫「資料需求申請表」經單位主管同意後，會辦資通安全小組，本校始得提供資料內容。

5.2 軟體控制措施

5.2.1 作業系統變更時，應審查與測試重要營運系統，以確保對組織作業或安全無不利之衝擊。

5.2.2 系統軟體安裝

5.2.2.1 系統軟體應由系統負責人進行安裝，安裝時應視狀況通知相關技術人員支援或通知使用者，以避免資訊服務中斷或影響業務。

5.2.3 系統軟體測試

5.2.3.1 軟體測試由系統負責人辦理，測試時應事先通知協調相關人員支援。

5.2.3.2 系統負責人應通知相關人員及使用者以避免資訊服務中斷或影響業務。

5.2.4 系統軟體更新

系統負責人需定期檢視更新系統安全修補、防毒軟體及防毒碼，以維持系統正常運作。

5.3 開發作業控制措施

5.3.1 提案與回覆

5.3.1.1 申請單位提出「系統需求申請與回覆單」敘明需求理由。

5.3.1.2 承辦人員於完成與申請單位之訪談與系統分析後，於「系統需求申請與回覆單」中回覆評估結果，包含功能細項、預估人力與時程、建議方案等。

5.3.1.3 經評估系統修改幅度不大，且不涉及系統流程變更者，於「系統需求申請與回覆單」中回覆處理結果並結案。

5.3.2 分析規劃與程式撰寫

5.3.2.1 程式開發者應於程式開發前進行系統分析，系統分析時應將系統安全需求納入考量。如涉及重要資料之傳輸，應使用 SSL 加密金鑰，並依下列規定管理金鑰：

5.3.2.1.1 金鑰應有明確的啟動與止動日期，並於可用期間，保護其不被修改、遺失和破壞。

5.3.2.1.2 金鑰之使用與存取，應限於使用金鑰之系統管理者，不可由其他非系統管理者任意存取。

5.3.2.1.3 對於金鑰之使用、啟動、止動，皆應留存相關之紀錄。

5.3.2.2 輸入應用系統之資料，應檢查主要欄位或資料檔案的內容，以確保資料的有效性及真確性。

5.3.2.3 對高敏感性的輸入資料，必要時應採用資料保密機制，在傳輸或儲存過程中應採加密方法保護。

5.3.2.4 輸出之資料，應於輸出之前，確認其正確性；對於系統內之訊息，則需保護其完整性。

5.3.3 測試

5.3.3.1 測試環境與線上環境應予以分開。

5.3.3.2 程式設計初步完成後，準備「系統測試記錄表」通知申請單位進行聯合測試，並請申請單位於「系統測試記錄表」中填寫測試結果。

5.3.3.3 程式功能若無法達成申請單位預定需求，則請系統開發人員另行修改程式後，擇期再測試，直至符合預定需求為止。

5.3.4 上線與驗收

5.3.4.1 聯合測試進行順利完成後，進行相關驗收作業，並請申請單位簽收「系統測試記錄表」。

5.3.4.2 若原系統已經存在，應於系統上線前訂定「系統上線及緊急復原計畫表」，內容包含系統轉換規劃，轉換備援處理等。

5.3.4.3 系統上線後，程式開發者應提出系統設計與功能規格書，內容包含系統作業流程圖、系統資料庫說明表、系統程式碼清冊。

5.3.4.4 系統若委由其他單位開發時，應請開發單位交付系統設計與功能規格書，由本校程式開發權責單位審閱，並留存備查。

5.3.5 後續系統增修維護

5.3.5.1 專案上線後功能如需修補，申請單位應填「系統需求申請與回覆單」，程式開發權責單位依需求規格進行訪談規劃設計。

5.3.5.2 程式開發權責單位完成系統增修作業後與申請單位進行測試驗收結案。

5.4 變更作業控制措施

5.4.1 變更作業應考量之事項：

5.4.1.1 在實際執行變更作業前，變更作業之細項建議，應取得權責單位主管人員之核准。

5.4.1.2 應確保系統變更作業不致影響或破壞系統原有的安全控制。

5.4.1.3 系統開發或變更，應更新系統文件。

5.4.1.4 程式維護時，應在程式內以註解說明異動部分。

5.4.1.5 所有系統變更作業請求，皆應建立紀錄供稽核運用。

5.4.2 變更作業之控制流程：

5.4.2.1 在實際執行變更作業前，申請者應先填具「系統需求申請與回覆單」提出變更需求，並經權責單位主管人員核准確認。

5.4.2.2 變更作業如有需要，應會辦相關人員配合。

5.4.2.3 上線前應先進行測試，必要時請相關人員配合建置測試環境。

5.4.2.4 除非事先經由權責單位主管人員核准外，測試不應在線上營運系統執行。

5.4.2.5 測試完成後，程式開發權責單位應擬定「系統上線及緊急復原計畫表」，決定上線日期，經權責單位主管人員確認後始得上線。

5.4.2.6 上線後應立即於線上營運系統再行測試，以確認系統運作正常。測試人員不宜與程式開發者為同一人，以減少錯誤機會發生。

5.4.2.7 上線後測試如發現狀況，應嘗試可否立即排除，如無法立即排除，應依緊急復原計畫，回復上線前原狀。

5.4.2.8 變更作業完成後應修改相關系統設計與功能規格書。

6 相關文件

6.1 通信與作業管理

6.2 資料需求申請表

6.3 系統需求申請與回覆單

附件12之附錄1

國立苑裡高級中學-系統開發與維護					
文件編號	NYLSH-ISMS-01-012	機密等級	限閱	版次	4.0

國立苑裡高級中學資料需求申請表

填表日期：　　年　　月　　日

系統別			
申請單位		連絡人及電話	
需求事申			
依據文件 請附文件影本			
需求範圍 （請詳列如學生科別、年級、學制、畢業年度）			
需求欄位 請詳列如學生學號、姓名、性別、戶籍地址、聯絡電話或提供範本格式			

申請單位 承辦人及主管簽章	資料權責單位 承辦人及主管簽章	資通安全小組 承辦人及主管簽章	申請單位簽收 承辦人及主管簽章

※資料僅供需求事由相關目的使用，不得任意提供他人或其他目的使用。

※需求資料內容如包含個人資料應遵守「個人資料保護法」指定專人依相關法令辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

附件12之附錄2

國立苑裡高級中學-系統開發與維護					
文件編號	NYLSH-ISMS-01-012	機密等級	限閱	版次	4.0

國立苑裡高級中學系統需求申請與回覆單

填表日期：　　年　　月　　日

需求申請說明			
系統名稱		希望啟用日期	年　　月　　日
作業現況	□未電腦化（□新增作業 或 □舊有人工作業） □已電腦化（需要 □新增功能 □修改功能 □重新設計系統） □系統開發中需求變更		
預期成效	使用年限：□一年內 □一至三年 □三至五年 □五年以上 使用頻率（作業週期）：_____人次/ □日 □月 □季 □學期 或 □年 其他成效指標：		
功能/流程描述	□詳細文案（共____頁）　　□參考資料 附件資料共____件		
申請人		主管	

需求申請回覆說明					
說明/可能影響範圍					
評估結果	□自行開發，可於期望時限內完成 □自行開發，無法於期望時限內完成 □尋求委外廠商　　□尋求_____協助 □不建議執行 補充說明：				
配合事項					
預計工時		預計交付測試日		預計上線日期	
系統上線及緊急復原計畫表紀錄編號：　　（若為系統變更請填上編號）					
承辦人		主管			

附件13

備　份　資　料　回　復　測　試　紀　錄　表

回復系統名稱	回復資料名稱	回復時間	測試人員	測試結果	清除資料
無線網路認證系統	整機資料回復	115/07/21	林晉逸	■正常(0 時 16 分) □不正常：_____	■資料庫（DataBase） ■資料表（Table） ■資料紀錄（Record） ■檔案（File）
				□正常(　時　分　) □不正常：_____	□資料庫（DataBase） □資料表（Table） □資料紀錄（Record） □檔案（File）

備註：請留存相關佐證紀錄做為附件。(如:備份/還原時間截圖、檢查回復資料截圖、清除資料截圖)

承辦人	主管

附件14

國立苑裡高級中學-資通安全事件通報應變程序					
文件編號	NYLSH-ISMS-01-014	機密等級	限閱	版次	4.0

1 目的

確保國立苑裡高級中學（以下簡稱本校）遵照資通安全事件通報應變及演練辦法，特制定本資通安全事件通報應變程序，以迅速有效獲知並處理事件。

2 適用範圍

發生於本校之事件，系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅者。

3 責任

3.1 本校於發現資通安全事件時，應依本程序或權責人員之指示，執行通報及應變事務。

3.2 本校應視必要性，與受託機關約定，使其制定其資通安全事件通報應變程序，並於知悉資通安全事件後向本校進行通報，於完成事件之通報及應變程序後，依本校指示提供相關之紀錄或資料。

3.3 本校應於知悉資通安全事件後，應依本程序之規定，儘速完成損害控制、復原與事件之調查及處理作業。完成後，應依教育部指定之方式進行結案登錄作業，並送交調查、處理及改善報告。

4 事件通報窗口及緊急處理小組

4.1 臺灣學術網路資通安全事件委託由臺灣學術網路危機處理中心之教育機構資安通報應變小組負責，聯繫聯絡電話：(07)525-0211、電子郵件：service@cert.tanet.edu.tw

4.2 本校應至少指派2位以上資安通報人員，並於「教育機構資安通報平台」登錄相關聯絡資料，如有異動亦應立即上網更新。

4.3 本校之資通安全事件通報窗口為緊急處理小組資訊媒體組長、聯繫專線(037)868680#801。

4.4 本校應以適當方式使相關人員明確知悉本機關之通報窗口及聯絡方式。

4.5 本校所屬人員知悉資通安全事件時，應立即至「教育機構資安通報平台」，進行通報登錄資通安全事件細節、影響等級及支援申請等資訊。

4.6 本校應確保通報窗口之聯絡管道全天維持暢通，若因設備故障或其他情形導致窗口聯絡管道中斷，該中斷情況若持續達1小時以上者，應即將該情況告知相關人員，並即提供其他有效之臨時聯絡管道。

4.7 事件發生之單位權責人員應與相關單位密切合作以進行事件之處理，並提供通報窗口適時掌握事件處理之進度及其他相關資訊。

4.8 事件經初步判斷認為可能屬重大資通安全事件（第三級、第四級）或事態嚴重時，應即向資安長報告，並進行處理。如接獲本校所屬單位或受託廠商所通報之資通安全事件時，亦同。

4.9 緊急處理小組成員由資安長指派機關之資通安全相關技術人員擔任，或亦得由其他機關資通安全相關技術人員或外部專家擔任之。

4.10各相關權責人員應紀錄事件處理過程，並檢討事件發生原因，著手進行改善，並留存必要之證據。

5 通報作業程序

5.1 判定事件等級之流程及權責

本校之權責人員或緊急處理小組應依據以下事項，於知悉資通安全事件後，依規定完成「資通安全事件通報應變及演練辦法」之資通安全事件等級判斷：

5.1.1 事件涉及核心業務或關鍵基礎設施業務之資訊與否。

5.1.2 事件導致核心業務資訊或核心資通系統遭竄改之影響程度，屬嚴重或輕微。

5.1.3 事件所涉資訊是否屬於國家機密或一般公務機密。

5.1.4 機關業務運作若遭影響或資通系統停頓，是否可容忍中斷時間內能回復正常運作。

5.1.5 事件其他足以影響資通安全事件等級之因素。

5.2 本校因網路或電力中斷等事由，致無法依前項規定方式為通報者，應於確認資通安全事件條件成立後1小時內，與所隸屬區縣市網路中心及教育機構資安通報應變小組聯繫，先行提供當次資通安全事件應通報之內容及無法通報依規定方式通報之事由，並於事由解除後，依原方式補行通報。

5.3 資通安全事件等級如有變更，本校權責人員或緊急處理小組應告知通

報單位，使其續行通報作業。

5.4 本校於委外辦理資通系統之建置、維運或提供資通服務之情形時，應於合約中訂定委外廠商於知悉資通安全事件時，應即向委託單位所屬之權責人員通知，以指定之方式進行通報。

5.5 本校於知悉資通安全事件後，如認該事件之影響涉及其他機關或應由其他機關依其法定職權處理時，本校權責人員或緊急處理小組應於知悉資通安全事件後1小時內，將該事件依教育部指定方式或主管機關指定「國家資通安全通報應變網站」通報。

5.6 本校執行通報應變作業時，得視情形向所隸屬區縣市網路中心人員提出技術支援或其他協助之需求。

6 應變程序

6.1 事件發生前之防護措施規劃

本校應於平時妥善實施資通安全維護計畫，並以組織營運目標與策略為基準，透過整體之營運衝擊分析，規劃業務持續運作計畫並實施演練，以預防資通安全事件之發生。

6.2 事件發生時之損害控制機制

6.2.1 負責應變之權責人員或緊急處理小組，應完成以下應變事務之辦理，並留存應變之紀錄

6.2.1.1 資通安全事件之衝擊及損害控制作業。

6.2.1.2 資通安全事件所造成損害之復原作業。

6.2.1.3 重大資通安全事件（第三級、第四級）相關鑑識及其他調查作業。

6.2.1.4 重大資通安全事件（第三級、第四級）之調查與處理及改善報告之方式。

6.2.1.5 重大資通安全事件（第三級、第四級）後續發展及與其他事件關聯性之監控。

6.2.1.6 資訊系統、網路、機房等安全區域發生重大事故或災難，致使業務中斷時，應依據本機關事前擬定之緊急計畫，進行應變措施以恢復業務持續運作之狀態。

6.2.1.7 其他資通安全事件應變之相關事項。

6.2.2 對於第一級、第二級資通安全事件，本校應於知悉事件後 72 小時內完成前項事務之辦理，並應留存紀錄；於第三級、第四級資通安全事件，本校應於知悉事件後 36 小時內完成損害控制或復原作業，並執行上述事項，及留存相關紀錄。

6.2.2.1 本校完成資通安全事件處理後，須至「教育機構資安通報平台」填報資通安全事件處理辦法及完成時間。

6.2.2.2 本校於知悉受託廠商發生與受託業務相關之資通安全事件時，應於知悉委外廠商發生第一級、第二級資通安全事件後 72 小時內，確認委外廠商已完成損害控制或復原事項之辦理；於知悉委外廠商發生第三級、第四級資通安全事件後 36 小時內，確認委外廠商完成損害控制或復原事項之辦理。

7 資通安全事件後之復原、鑑識、調查及改善機制

7.1 本校發生資通安全事件時，應時限內完成資通安全事件之通報及應變程序，針對事件所造成之衝擊、損害及影響進行調查及改善，於事件發生後 1 個月內完成資通安全事件調查、處理及改善報告。

7.2 資通安全事件調查、處理及改善報告，依「資通安全管理法施行細則」第 12 條規定應包括以下項目：

7.2.1 事件發生或知悉其發生、完成損害控制或復原作業之時間。

7.2.2 事件影響之範圍及損害評估。

7.2.3 損害控制及復原作業之歷程。

7.2.4 事件調查及處理作業之歷程。

7.2.5 事件根因分析。

7.2.6 為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。

7.2.7 前款措施之預定完成時程及成效追蹤機制。

7.3 本校應向所隸屬之上級機關及教育部提出前項之報告，以供監督與檢討。

8 事件相關紀錄之保全

8.1 本校應將資通安全事件之通報與應變作業之執行、事件影響範圍與損害程度以及其他通報應變之執行情形，於「教育機構資安通報平台」上填報完整之紀錄。

8.2 本校於完成資通安全事件之通報及應變程序後，應依據實際處理之情形，於必要時對本管理程序、人力配置或其他相關事項進行修正或調整。

9 事件發生前之演練作業

9.1 本校依據「資通安全事件通報應變及演練辦法」之規定所辦理之社交工程演練並紀錄於「社交工程演練結果統計表」及資通安全事件通報及應變演練。

9.2 本校應配合教育部、教育部國民及學前教育署或主管機關依據「資通安全事件通報應變及演練辦法」之規定所辦理之下列資通安全演練作業：

9.2.1 社交工程演練。

9.2.2 資通安全事件通報及應變演練。

9.2.3 網路攻防演練。

9.2.4 情境演練。

9.2.5 其他資安演練。

10 相關文件及網站

10.1社交工程演練結果統計表

10.2教育機構資安通報平台（網址：https://info.cert.tanet.edu.tw）。

10.3國家資通安全通報應變網站（網址：https://www.ncert.nat.gov.tw/index.jsp）。

國立苑裡高級中學社交工程演練結果統計表

演練期別	社交工程 郵件 開啟率	社交工程 郵件 連結點閱率	社交工程 郵件 附件開啟率
114年上半年	14.29%	8.57%	8.57%
114年下半年	2.86%	0%	0%

資安承辦人　　資安執行秘書　　資安長

附件15

國立苑裡高級中學委外廠商資安管理作業自評表

填表日期：　　年　　月　　日

委外廠商名稱		委外廠商 負責人	
專案名稱		單位/專案負責人	

評估項目	辦理情形
1.管理面	
1.1辦理本專案受託業務相關程序及環境之資通安全管理措施或通過第三方驗證	□辦理本專案受託業務之相關程序及環境已(將)通過_____認(驗)證並持續有效，驗證公司為_____ □辦理本專案受託業務之相關程序及環境已具備完善資安管理措施，詳_____文件(如未載明於既有文件內，請於備註欄內說明相關措施) □本專案受託業務之相關程序及環境未導入適當資安管理措施 備註：_____
1.2本專案之資安負責人、資安專責主管或其他資安人員之人力配置規劃	□本專案之資安負責人(專案主管)為____ □本專案之資安人員為____ □本專案未指派資安負責人、資安專責主管或其他資安人員 備註：_____
1.3本專案之資安風險評估，包含可能之資通系統機密性、完整性、可用性風險，及採取之對應控制措施	□本專案受託業務相關程序及環境之資安風險評估結果已(將)載明於____文件，已(將)採取對應之控制措施詳____文件(如未載明於既有文件內，請於備註欄內說明相關措施) □未就本專案進行資安風險評估 備註：_____

1.4本專案範圍內之資通安全事件通報應變程序，包含知悉資通安全事件發生或有發生之虞之相關通報時效規定、通報方式、資通安全事件調查、處理及改善流程	□本專案受託業務相關程序及環境之資通安全事件通報應變程序已(將)載明於_____文件(如未載明於既有文件內，請於備註欄內說明相關措施)，知悉資通安全事件或發現有事件發生之虞時，應於__小時內向甲方等相關利害關係人通報，通報對象包含____ □未就本專案訂定相關資通安全事件通報及應變程序 備註：_____
1.5由招標公告日起算，過去3年是否發生因管理議題肇因之重大資通安全事件	□過去3年無發生因管理議題肇因之資通安全事件 □是，共__次，事件發生主要根因為____ 備註：_____
2.技術面	
2.1本專案範圍內之資通系統，包含主要履約標的之資通系統及其他執行本專案業務所需使用之業務、行政相關資通系統，辦理安全性檢測	□本專案範圍內之資通系統將規劃執行_____(如源碼掃描、弱點掃描、滲透測試)，檢測項目及本案範圍為：_____ □未就本專案範圍內之資通系統規劃安全性檢測 備註：_____
2.2辦理本專案受託業務環境及設備導入之相關資通安全防護措施	□本專案受託業務之環境及設備已(將)導入(啟用)_____(如防毒軟體、防火牆、電子郵件過濾機制、入侵偵測及防禦機制等)，導入項目及本案範圍為：_____ □本專案受託業務之環境及設備未導入相關資通安全防護措施 備註：_____
2.3本專案範圍內之資通系統及專案資料之存取控制等權限管理機制，如 PM、系統管理員、一般使用者帳號之權限分級原則及控管方式	□本專案範圍內之資通系統帳號或使用者權限分成__種等級，相關存取控制、權限管理機制說明如下：____ □未規劃本專案範圍內之資通系統及專案資料相關存取控制及權限管理機制 備註：_____
3.認知訓練面	
3.1本專案直接履約相關人員之資安教育訓練	□本專案直接履約相關人員之資安教育訓練包含__小時之資安通識教育訓練，對象包含____；__小時之資安專業教育訓練，對象包

	含____ □未規劃相關資安教育訓練 備註：_____
3.2本專案團隊人員取得之資通安全專業證照	□本專案具資安證照之團隊成員有：__位 □本專案團隊人員未具備資通安全專業證照 備註：_____

廠商用印：

附件16

國立苑裡高級中學委外廠商保密同意書

茲緣於簽署人為 _____ (廠商名稱，以下稱廠商)之負責人，本公司負責《學校全銜》(以下簡稱本校）_____（資通業務案名，以下稱「本案」)，本案為□核心業務□非核心業務(請勾選)，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、 本校配合教育部五大核心資通系統向上集中，爰資通安全責任等級為D級，本案資通系統防護需求等級為□普 □中 □高(請勾選)。簽署人承諾於本契約有效期間內配合教育部、教育部國民及學前教育署、本校各項資通系統防護作業，並依據資通安全管理法及子法、個人資料管理法及施行細則等，進行本案各項工作，以符合法遵。

第二條、 簽署人應主動了解本案防護等級，並遵守本校相關法令及規範，如「資通安全政策」等。

第三條、 簽署人承諾於本契約有效期間內及本契約期滿或終止後，依本校指示將其製造產品或複製品進行返還、移交、刪除或銷毀作業；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。

第四條、 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。

第五條、 簽署人在下述情況下解除其所應負之保密義務：

一、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。

二、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。

三、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，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連帶賠償責任。

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、 本同意書一式叁份，本校、簽署人及.....（廠商）各執存一份。

簽署人姓名及簽章：

簽署人住址：

聯絡電話：

廠商名稱、住址及公司章：

中　　華　　民　　國　　年　　月　　日

附件17

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，處理《學校全銜》(以下簡稱本校)
_____（資通業務)，謹聲明恪遵本校下列工作規定，並對工作中所持有、知悉之資通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。

第一條、 應主動了解本校資安責任等級，並依該項業務之防護等級進行各項工作。

第二條、 應主動了解並遵守本校相關法令及規範，如「資通安全政策」等。

第三條、 未經申請核准，不得私自將本校之資通設備、媒體檔案及公務文書攜出。

第四條、 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通設備連接本校網路。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。

第五條、 經核准攜入之資通設備欲連接本校網路或其他資通設備時，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。

第六條、 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。本校得定期或不定期派員稽核立切結書人是否符合上列工作規定。

第七條、 本保密切結書不因立切結書人離職而失效。

第八條、 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：

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

廠商負責人聯絡電話及地址

中　　華　　民　　國　　年　　月　　日

附件18

國立苑裡高級中學委外廠商查核暨自我檢核項目表

填表日期：　　年　　月　　日

委外廠商名稱		委外廠商負責人			
專案名稱		單位/專案負責人			
查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
管理面	1.1 辦理合約標的系統程序及環境是否進行合適控管？ □具 ISO27001認證 □不具 ISO27001認證，但有 □進行資通系統盤點 □進行資通系統風險評估 □有防火牆且有管控規則 □有日誌管理 □有合適權限管控	□	□		
	1.2 乙方是否有符合人員及設備安全評估措施？ □人員不得為陸籍 □設備不得為大陸地區廠商之產品	□	□		
	1.3 是否簽署委外廠商保密同意書、委外廠商執行人員保密切結書 □委外廠商保密同意書 □委外廠商執行人員保密切結書	□	□		
	1.4 是否知悉甲方資通安全責任等級：_____級？	□	□		
	1.5 是否知悉合約標的系統為□核心 □非核心 資通系統，並依據「資通安全責任等級分級辦法」執行系統防護需求等級之相關防護控制措施附表十、資通系統防護基準：資通系統防護基準為□普 □中？	□	□		

	1.6 是否了解甲方資通安全維護計畫對合約標的系統各項要求？	□	□	＼	
	1.7 是否配合甲方每年辦理1次業務持續運作演練及1次資通安全事件通報演練？	□	□	＼	
技術面	2.1 合約標的系統是否符合資通系統防護基準規定控制措施？	□	□	＼	
	2.2 合約標的系統是否具備合適備份機制？	□	□	＼	
	2.3 合約標的系統是否記錄事件、日誌紀錄管理，如：保留日誌至少6個月、記錄特定事件功能、記錄系統管理者執行各項功能等？	□	□	＼	
	2.4 參考本表第1.5項或乙方填復「委外廠商資安管理作業自評表」 2.4.1 合約標的系統是否完成弱點掃描，並完成修補中級(含)以上之風險？	□	□	□	
	2.4.2 合約標的系統是否完成第3方軟體、服務、函式庫或其他元件掃描，並完成修補中級(含)以上之風險？	□	□	□	
	2.4.3 合約標的系統是否完成滲透測試，並完成修補中級(含)以上之風險？	□	□	□	
	2.4.4 合約標的系統是否完成源碼檢測，並完成修補中級(含)以上之風險？	□	□	□	
認知訓練	3.1 是否參加「e等公務園+學習平臺」或「臺北 e 大」或專業訓練單位或學校自辦 3小時以上資通安全教育訓練？	□	□	＼	

廠商名稱、住址及公司章：

附件19

國立苑裡高級中學資通安全教育訓練統計表

人員類別	課程時數規定	應上課人數	完成人數	完成百分比（完成人數/應上課人數）
資通安全人員	每年完成12小時以上資通安全專業課程訓練或資通安全職能訓練。	1	1	100%
資通安全人員以外之資訊人員註1	每2年完成3小時以上資通安全專業課程訓練或資通安全職能訓練且每年完成3小時以上資通安全通識教育訓練。	1	1	100%
一般使用者及主管	每年完成3小時以上資通安全通識教育訓練。	103	103	100%

註1：資訊人員泛指機關資訊單位所屬人員，或業務單位所屬人員並從事資通系統自行或委外設置、開發、維運者，例如：系統管理者、系統承辦人、擁有系統後台管理權限之人員等。

資安承辦人　　資安執行秘書　　資安長

附件20

國立苑裡高級中學-內部稽核計畫					
文件編號	NYLSH-ISMS-01-020	機密等級	限閱	版次	4.0

1 主旨

為落實國立苑裡高級中學（以下簡稱「本校」）資通安全維護計畫執行，以反映政策、法令、技術及現行業務之最新狀況，確保資通安全政策與資訊安全實務作業之有效性及可行性。

2 目標

符合本校所訂定之資通安全政策及各項安全管理規定。

3 稽核範圍

本校行政單位資安事項與行政人員電腦使用情形。

4 稽核項目

4.1 行政單位資通系統或服務委外辦理之管理。

4.2 行政人員資安認知情形（含保密切結與安全守則）。

4.3 資通設備是否有合適安全控管措施。

4.4 重要資產、個人資料或個人資料檔案存放地點是否符合安全控管措施。

5 資通安全稽核小組成員

組長：秘書○○○

組員：主任○○○、組長○○○

6 稽核時程

時 間	項 目	稽核人員	地點
09:00-09:30	啟始會議		
09:30-10:30	1 行政單位資通系統或服務委外辦理之管理。 2 行政人員資安認知情形（含保密切結與安全守則）。 3 資通設備是否符合安全控管措施。 4 重要資產或、個人資料或個人資料檔案存放地點是否符合安全控管措施。	秘書○○○ 主任○○○ 組長○○○	資通安全事件發生單位

時　間	項　　目	稽核人員	地點
10:30-11:00	稽核結果彙整		
11:00-11:30	結束會議		

7　稽核程序

7.1 執行日期：本校發生資通安全事件後，針對發生資通安全事件之單位進行內部稽核，應於1個月內完成實地稽核及資通安全事件調查、處理及改善報告。

7.2 啟始會議

7.2.1 確認稽核目的及範圍

7.2.2 稽核程序報告

7.2.3 稽核方法說明

7.3 實地稽核

7.3.1 實地驗證資訊安全管理系統執行之有效性

7.3.2 以面談、觀察、抽樣檢查方式進行

7.4 稽核結果彙整

7.4.1 資通安全稽核小組根據稽核事實討論所發現之缺失事項

7.4.2 彙整稽核結果

7.4.3　總結報告

7.5 結束會議

7.5.1 資通安全稽核小組報告發現之缺失事項

7.5.2 改善建議

7.5.3 問題澄清與討論

7.5.4 稽核總結

8　相關文件

8.1 稽核項目紀錄表

8.2 矯正與預防處理單

附件21

國立苑裡高級中學稽核項目紀錄表

受稽單位：　　受稽日期：　　年　　月　　日

稽核項目	稽核內容	稽核結果			說　　明
		符合	不符合	不適用	
1.資通安全責任	1.1. 知悉學校資安等級？	□	□	＼	
	1.2. 知悉負責系統之防護基準？	□	□	＼	
	1.3. 具每年3小時資安通識教育訓練	□	□	＼	
	1.4. 簽署員工安全守則及保密切結書	□	□	＼	
2.資通訊設備安全控管措施	2.1. 具高強度登入密碼	□	□	＼	
	2.2. 有定期更新密碼	□	□	＼	
	2.3. 設置螢幕保護程式	□	□	＼	
	2.4. 安裝學校防毒程式	□	□	＼	
	2.5. 有開啟系統防火牆	□	□	＼	
	2.6. 未安裝盜版軟體或不合宜授權軟體	□	□	＼	
3.重要資產或個資資料管控措施	3.1. 重要資產或個資資料有上鎖	□	□	□	
	3.2. 重要資產或個資資料區域具鑰匙控管措施	□	□	□	
4.資通訊系統契約內容	4.1. 資通訊系統契約具合適之資安條款	□	□	□	
	4.2. 廠商簽署委外廠商保密同意書、委外廠商執行人員保密切結書	□	□	□	
	4.3. 廠商簽署委外廠商查核暨自我檢核項目表	□	□	□	

承辦人		主管	
稽核人員		稽核組長	

附件22

國立苑裡高級中學內部稽核報告

1 稽核目的

為落實及國立苑裡高級中學（以下簡稱「本校」）執行資訊安全管理制度之成效，以確保資通安全政策、法令、技術及現行作業之有效性及可行性。

2 稽核範圍

本校行政單位資安事項與行政人員電腦使用情形。

3 稽核項目

3.1 行政單位資通系統或服務委外辦理之管理。

3.2 行政人員資安認知情形(含保密切結與安全守則)。

3.3 資通設備是否符合安全控管措施。

3.4 重要資產或個資資料存放地點是否符合安全控管措施。

4 資通安全稽核小組

組長：秘書○○○

組員：主任○○○、組長○○○

主導稽核員：○○○

5 稽核日期：　　年　　月　　日

6 稽核期間：自　　年　　月　　日至　　年　　月　　日

7 稽核結果及其他建議事項

項次	稽核項目	稽核發現	建議事項
1			
2			
3			
4			

其他建議事項

8 缺失矯正與預防處理

受稽部門於接獲稽核報告後，應依據「矯正預防措施管理」之規定，最晚於10個工作天內將該單位之缺失分析原因及擬採行之矯正與預防措施填列於「矯正與預防處理單」內，且經單位主管核定後回覆資通安全稽核小組。

附件23

國立苑裡高級中學矯正與預防處理單

<table>
<tr><td>提出單位</td><td></td><td>提出人員</td><td></td><td>提出日期</td><td></td></tr>
<tr><td>處理單位</td><td></td><td>處理人員</td><td></td><td>事件人員</td><td></td></tr>
<tr><td>事件分類
（外部稽核）</td><td colspan="2">□主要不符合事項 □觀察事項
□次要不符合事項 □建議事項</td><td>事件來源</td><td colspan="2">□內部稽核 □外部稽核
□資通安全事件 □自行提出
□其他</td></tr>
<tr><td>問題或不符合事項說明</td><td colspan="5"></td></tr>
<tr><td>原因分析</td><td colspan="5"></td></tr>
<tr><td rowspan="6">矯正與預防措施評估</td><td colspan="5">暫時性對策：（控制不符合事項的擴大或消除單一事件的影響）</td></tr>
<tr><td>預訂完成日期</td><td></td><td>追 蹤 人</td><td colspan="2"></td></tr>
<tr><td>追 蹤 日 期</td><td></td><td>確認結果</td><td colspan="2"></td></tr>
<tr><td colspan="5">長期性對策：（消除不符合事項或潛在風險的根本原因，防止類似事件發生）</td></tr>
<tr><td>預訂完成日期</td><td></td><td>追 蹤 人</td><td colspan="2"></td></tr>
<tr><td>追 蹤 日 期</td><td></td><td>確認結果</td><td colspan="2"></td></tr>
</table>