國立花蓮特殊教育學校

112 年度第 2 次資訊安全管理審查會議紀錄

壹、 時　間：112 年 3 月 21 日(星期二)　15 時 00 分
貳、 地　點：第一會議室
參、 主　席：馬心正校長　　記錄：設備組林燕忠
肆、出　席：林佩真主任、劉志城主任、孫聖翔主任、曾張旅主任、蘇麗英主任、陳曉娟主任、胡齊峰幹事、張人方書記、高啟森技士、胡禧年組員、林燕忠組長。

伍、報告事項

一、修正本校資資訊安全組織成員表成員，新增秘書 1 人，成員表如附件。

二、國教署定期辦理資安認知宣導教育訓練，並要求校內 2 名以上人員參加，由各處室資訊安全組織成員輪替代表參加，以提升校內人員資通安全能力(3 月 3 日教育訓練由學務處、教務處代表參加)。

三、本校學校網站經教育單位弱點檢測平台(EVS),2 月 15 日檢測結果，高風險、中風險數量為零，低風險數量為 1，檢測結果請參閱附件。

四、因應學校個人電腦、筆記型電腦數量已超出學校原有採購防毒軟體授權數 ，已於 111 年 1 月 4 日採購電腦防毒軟體授權(授權數量 500 台，授權 5 年)，請各處室資訊安全小組成員，協助檢視處室資訊設備，是否已安裝防毒軟體，並正確啟動。(本案已建立矯正與預防處理單，並完成追蹤改善處理情形)。

五、本校資訊機房巡檢紀錄 112 年 1 月至 3 月如附件，請參閱，其中有發現應機房濕度有過高及 UPS 不斷電設備故障情形，於報告事項第六、七點說明處理情形。

六、因應機房濕度有過高狀況，已另採購品質較佳濕度計進行檢測，

已獲得較準確數值,經機房巡查結果,機房溼度大多正常範圍(溼度會有 1、2 日顯示超出 60%),將另行安裝除濕機供機房使用。(本案已建立矯正與預防處理單，並完成追蹤改善處理情形) 。

七、機房巡查時,發現舊有 UPS 不斷電設備故障情形，已另行採購，進行設備汰舊更新。(本案已建立矯正與預防處理單，並完成追蹤改善處理情形) 。

陸、討論事項

案號一

案由：111年度校園資通安全業務管理輔導團實地訪視「綜合意見」，矯正與預防處理單，追蹤改善處理情形，提請討論。

說明：

一、 依據依據111年9月14日111年度校園資通安全業務管理輔導團實地訪視「綜合意見」第2項「應依照資安維護計畫，將稽核缺失做成矯正與預防處理單，以落實追蹤改善機制。」,將實地訪視之稽核意見失做成矯正與預防處理單，落實追蹤改善情形。

二、 稽核缺失做成矯正與預防處理單，共15件，其中8件已於112年第1次資訊安全管理審查會議確認完成追蹤改善。

三、 本次會議針對矯正與預防處理單1111221-08(資安教育訓練)、1111221-14(電腦掃毒排程)、1111221-15(機房區域網路隔離) 追蹤改善情形。

決議：

一、矯正與預防處理單1111221-14(電腦掃毒排程)、1111221-15(機房區域網路隔離)已完成。

二、矯正與預防處理單1111221-08(資安教育訓練)預定本年度9月辦理資通安全教育訓練。

案號二

案由：審查本校112年度本校資訊資產清單，並對資訊資產風險評估進行檢視。

說明：

一、 依據本校資訊資產管理程序書辦理。

二、 為落實資訊資產管理，檢視資訊資產分類分級及價值之結果是否適當及高風險之資訊資產是否採取相應之控制措施。

決議：

一、已完成資訊資產清單如附件。

二、請各處室完成資訊資產風險評估，於4月22日召開第3次資審會，再進行檢視。

案號三

案由：為遵循資訊資產管理及防範個人資料外洩，針對校內資訊設備儲存之資料清除方式，提請討論。

說明：

一、依據本校資訊資產異動作業說明書，硬體及通訊資訊資產新增、異動、報廢時，應填寫資訊資產異動申請表。

二、儲存媒體報廢清除方式參考如下：

1. **硬碟：**
   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。
2. **光碟：**
   於光碟表面塗抹層製造刮痕後，再進行絞碎作業。
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。

決議：本校資訊資產新增、異動、報廢時，應填寫資訊資產異動申請表。

案號四

案由：依據國教署111年國立高級中等以下學校資通安全實地稽

核訪視及資通安全維護計畫實施情形書面審查之共通性問題及分析建議，針對本校資通安全管理作業進行改善，提請討論。

說明：

一、依據112年3月16日臺教國署資字第1120037276號函。

二、實地稽核訪視學校不符合項目共通性問題統計、資通安全維護計畫實施情形書面審查結果學校不符合項目共通性問題統計，如附件。

決議： 依來函分析建議，學校辦理情形如下，再請各處室配合辦理。

(一)資通安全維護計畫實施情形書面審查結果分析建議。

資通安全維護計畫實施分析建議	學校辦理情形
1、多數學校無法完成資通安全健診與具備相關專業資安證照或認證，期待上級協助與指導。	配合上級辦理。
2、學校應針對校內資訊資產進行清查(包含明確的管理者及使用者)，並進行資訊資產風險評估，且針對高風險之資訊資產採取相應之控制措施。	已於112.03.21完成112年資訊資產清冊，於4月22日召開第3次資審會，進行資訊資產風險評估檢視。
3、學校應定期辦理資通安全認知宣導及教育訓練，應確實辦理與落實評量機制。	112年資通安全教育訓練，預定8月期初辦理。
4、學校之備份資料應定期進行回復測試，以確保備份資料之有效性。	校內相關系統的資料應進定期進行回復測試。
5、學校應落實針對委外資訊系統或維護合約中廠商所承諾工作內容進行檢核、履約督導及管理。	校內委外資訊系統，應與簽定合約並進行檢核，應完成填寫委外廠商查核項目表、委外廠商執行人員保密切結書、委外廠商執行人員保密同意書、備份狀況紀錄表等。
6、學校資通安全政策文件應由管理階層審核並發佈轉知全體同仁。	1112年資通安全政策，已112.01.13資審會討論通過，資通安全政策、計畫已公告校園網站、並於行政會報及全校教師會議中宣導報告。
7、學校之系統帳號應落實盤點並進行權限複檢，以確保資訊系統之安全。	於112.04.25召開第3次資審會進行檢視。
8、學校之資訊機房安全設備應定期查檢，同	1.資訊機房定期進行檢視。

仁應進行適當的設備使用訓練。	2.各處室資訊安全小組成員參加相關資安研習訓練。
9、學校應訂定內部稽核計書並落實定期內部稽核活動,以檢視校內資通安全活動之落實狀況。	修訂本校資通安全維護計劃(無辦理內部稽核)，配合資安責任等級分級辦法，辦理D級單位應辦事項。

（二）實地稽核訪視結果，共通性問題統計分析建議。

實地稽核訪視結果分析建議	學校辦理情形
1、學校系統帳號應落實盤點並進行權限複檢，以確保資訊系統之安全。	於112.04.25召開第3次資審會進行檢視。
2、學校應落實校內資訊資產進行清查(包含明確的管理者及使用者)，並針對資訊 資產進行資訊資產風險評估，且針對高風險之資訊資產採取相應之控制措施。	已於112.03.21完成112年資訊資產清冊，於112.04.25召開第3次資審會，進行資訊資產風險評估檢視。
3、學校針對資通系統委外應與廠商簽訂契約或協議書，契約或協議書應針對資通 系統防護進行協議，且應落實對委外廠商之履約檢核、督導管理及保密切結之簽署。	校內委外資訊系統，應與簽定合約並進行檢核，應完成填寫委外廠商查核項目表、委外廠商執行人員保密切結書、委外廠商執行人員保密同意書、備份狀況紀錄表等。
4、多數C級學校無法完成資通安全健診與具備相關專業資安證照或認證，期待上級協助與指導。	配合上級辦理。
5.確保學校所提供或使用的網路服務，避免受到任何未經授權的存取，需要採取控管作法，確保網路本身和使用者在利用時，不會發生安全上的問題，危害到學校的整體營運；如外部連線的使用者鑑別、網路設備鑑別、遠端診斷與組態埠保護、網路區隔、網路連線控制與網路路由控制等。	1.本校機房設備與校內一般使用者，區分不同網段，以降低未經授權存取之風險。 2.校園無線網路設定個人使用帳密，避免未經授權者使用。 3.本校建置整合式的防火牆，將交換器、無線基地台等網路相關設備統一納管及監控。
6、學校應針對備份資料定期進行回復測試，以確保備份資料之有效性。	校內相關系統的資料應進定期進行回復測試。
7、學校應訂定內部稽核計書且落實定期內部	本年度將邀請外部單位(東華大華區網中心或花蓮區資安輔導學

稽核活動，並應針對稽核活動缺失進行改善，以確保校內資通安全防護之落實。	校)，協助辦理內部稽核。
8、學校應定期召開管理審查會議並討論相關議題。	本校已配合定期召開資審會(本年度已於112.01.13、113.03.21召開2次資審會，112.04.25召開第3次資審會)
9、學校應針對資訊機房安全設備定期查檢，同仁並應進行適當的設備使用訓練。	1.資訊機房定期進行檢視。 2.各處室資訊安全小組成員參加相關資安研習訓練。
10、學校應定期取得系統弱點的資訊並進行系統漏洞修補，且點進行風險評估並進而採取必要管控及處理措施	1.校內資訊系統定期更新，確保資訊安全。 2. 於112.04.25召開第3次資審會，進行資訊資產風險評估檢視。

附件　　國立花蓮特殊教育學校

資訊安全組織成員表

職務	職稱
資訊安全委員會(資訊安全暨個人資料保護推動委員會)	
召集人	校長
委員	秘書
委員	教務主任
委員	學務主任
委員	總務主任
委員	實習主任
委員	人事主任
委員	主計主任
資訊安全官	
資訊安全官	校長
資訊安全執行秘書	
資訊安全執行秘書	設備組
資訊安全小組	
組長	教務主任
組員	設備組
組員 (資通安全情資之分類評估)	資訊技佐
組員	總務處書記
組員	學務處幹事

組員	實輔處技士
組員	人事室主任
組員	主計室組員
緊急處理組	
組長	教務主任
組員	學務主任
組員	總務主任
組員	實習主任
組員	人事主任
組員	主計主任

附件　教育單位弱點檢測平台(EVS)，2月15日檢測報告。

Scan of www.hlmrs.hlc.edu.tw

Scan details

Scan information	
Start time	2023-02-15T00:05:45.154244+08:00
Start url	https://www.hlmrs.hlc.edu.tw
Host	www.hlmrs.hlc.edu.tw
Scan time	140 minutes, 13 seconds
Profile	Full Scan
Server information	nginx/1.20.1
Responsive	True
Server OS	Unknown
Application build	15.2.221208162

Threat level

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alerts distribution

Total alerts found	10
High	0
Medium	0
Low	1
Informational	9

附件　資訊資產異動申請表

填表日期：　　年　　月　　日

項次	異動別	資產編號	資產類別	資 產 名 稱	使用單位	管理單位	資產價值	異 動 說 明	儲存資料銷毀清除
一								新增□ 異動□. 報廢□	□是　□否
二								新增□ 異動□. 報廢□	□是　□否
三								新增□ 異動□. 報廢□	□是　□否
四								新增□ 異動□. 報廢□	□是　□否
五								新增□ 異動□. 報廢□	□是　□否
六								新增□ 異動□. 報廢□	□是　□否

*資產類別：通訊（CM）、資料（DA）、文件（DC）、環境（EV）、硬體（HW）、軟體（SW）

使用單位		處室主管		資訊安全官	

資通安全維護計畫實施情形書面審查結果

學校不符合項目共通性問題統計

資安責任等級C級各校「不符合」項目共通性問題排序

排序	查核內容	不符合學校數
1	15.2 滲透測試	51
2	15.4 網路惡意活動檢視	45
3	15.5 使用者端電腦惡意活動檢視	45
4	15.6 伺服器主機惡意活動檢視	45
5	15.7 目錄伺服器設定及防火牆連線設定檢視	45
6	15.8 資通安全弱點通報機制	45
7	15.3 網路架構檢視	44
8	10.3 是否辦理委外廠商查核？	35
9	14.5 業務持續運作演練	34
10	10.2 監督受託者資通安全維護情形應注意事項	23
11	16.1 資通安全專職人員	21

資安責任等級D級各校「不符合」項目共通性問題排序

排序	查核內容	不符合學校數
1	10.3 是否辦理委外廠商查核？	14
2	13.1 資通安全維護計畫實施情形之稽核機制	8
3	13.2 資通安全維護計畫之持續精進及績效管理	7
4	9.1 資通安全情資之評估及因應措施 ？	6
5	6.1 資通安全風險評估及因應 ？	5
6	16.1 一般使用者及主管	5
7	4.2 經費之配置	4
8	7.1 資通安全防護及控制措施	4
9	10.1 選任受託者應注意事項	4
10	10.2 監督受託者資通安全維護情形應注意事項	4

83 校維護計畫實施情形書面審查結果，學校共通性問題統計分析建議：

1、多數學校無法完成資通安全健診與具備相關專業資安證照或認證，期待上級協助與指導。

2、學校應針對校內資訊資產進行清查(包含明確的管理者及使用者)，並進行資訊資產風險評估，且針對高風險之資訊資產採取相應之控制措施。

3、學校應定期辦理資通安全認知宣導及教育訓練，應確實辦理與落實評量機制。

4、學校之備份資料應定期進行回復測試，以確保備份資料之有效性。

5、學校應落實針對委外資訊系統或維護合約中廠商所承諾工作內容進行檢核、履約督導及管理。

6、學校資通安全政策文件應由管理階層審核並發佈轉知全體同仁。

7、學校之系統帳號應落實盤點並進行權限複檢，以確保資訊系統之安全。

8、學校之資訊機房安全設備應定期查檢，同仁應進行適當的設備使用訓練。

9、學校應訂定內部稽核計畫並落實定期內部稽核活動，以檢視校內資通安全活動之落實狀況。

實地稽核訪視

學校不符合項目共通性問題統計

排序	查核內容	不符合學校數
1	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？	46
2	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？	42
3	10.2 是否落實檢核及履約督導管理？	38
4	10.1 資通系統委外(含委辦)是否簽訂協議書或契約？	35
5	3.3 是否具備相關專業資安證照或認證？(本項C級機關列入評分，D級機關不列入評分)	33
6	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？	33
7	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？	29
8	4.1 是否建立資訊及資通系統資產目錄，並隨時維護更新？(本項將列為實地稽核重點項目，並納入機關(校長)考核參考)	26
9	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？	25
10	9.3 是否定期召開持續改善之管理審查會議？	24
11	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？	23
12	5.19 是否定期執行各項系統漏洞修補程式？	22
13	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？	22
14	10.3 委外(含委辦)相關人員是否簽訂保密合約書？	22
15	11.2 是否每兩年辦理一次資通安全健診？(本項C級機關列入評分，D級機關不列入評分)	21

76 校實地稽核訪視結果，共通性問題統計分析建議：

1、學校系統帳號應落實盤點並進行權限複檢，以確保資訊系統之安全。

2、學校應落實校內資訊資產進行清查(包含明確的管理者及使用者)，並針對資訊資產進行資訊資產風險評估，且針對高風險之資訊資產採取相應之控制措施。

3、學校針對資通系統委外應與廠商簽訂契約或協議書，契約或協議書應針對資通系統防護進行協議，且應落實對委外廠商之履約檢核、督導管理及保密切結之簽署。

4、多數C級學校無法完成資通安全健診與具備相關專業資安證照或認證，期待上級協助與指導。

5、確保學校所提供或使用的網路服務，避免受到任何未經授權的存取，需要採取

控管作法，確保網路本身和使用者在利用時，不會發生安全上的問題，危害到學校的整體營運；如外部連線的使用者鑑別、網路設備鑑別、遠端診斷與組態埠保護、網路區隔、網路連線控制與網路路由控制等。

6、學校應針對備份資料定期進行回復測試，以確保備份資料之有效性。

7、學校應訂定內部稽核計書且落實定期內部稽核活動，並應針對稽核活動缺失進行改善，以確保校內資通安全防護之落實。

8、學校應定期召開管理審查會議並討論相關議題。

9、學校應針對資訊機房安全設備定期查檢，同仁並應進行適當的設備使用訓練。

10、 學校應定期取得系統弱點的資訊並進行系統漏洞修補，且針對系統弱點進行風險評估並進而採取必要管控及處理措施。