壹、 會議時間：中華民國 110 年 3 月 23 日

貳、 會議地點：圖書館 3 樓會議室

參、 會議主席：陳香妘

肆、 出席人員：詳簽到表
列席人員：詳簽到表

伍、 會議記錄：

陸、 會議主題：110 年度第 1 次資通安全管理審查會議

柒、 報告及宣導事項

本次會議係依本校資通安全組織程序書規定「資通安全委員會應每年至少召開一次管理審查會議，得併同行政會議召開...」略以，爰併同本次會議召開。

一、 依國發會規定各機關對外提供之可編輯文件格式應採 ODF 文件格式，禁止使用 Office 商用文件(如 word、excel 等)，故官網公告之附件以及公文發文附件，請務必轉檔為 PDF 或 ODF 文件格式。

另，考量版權及為鼓勵學生使用 ODF 編輯軟體，學校所提供學生使用之公用電腦不會安裝微軟 Office 軟體。

二、 已確認國教署將於今年 4~10 月(待正式公文)稽核本校資安作業，將由國教署副署長主持，政風處進行稽核，屆時應該會抽測使用者電腦，故請所有人員務必遵守以下規範，實際稽核前會再宣導：

1. 本校相關資安公告皆依規定公布於「學校官網>行政單位>圖書館>資訊安全專區」。

2. 個人電腦依安裝學校要求之防毒軟體，並定期更新系統。

3. 個人電腦應設定登入密碼，密碼至少 8 碼，且須包含英文字母大小寫及數字，超過 15 分鐘不使用時應自動鎖定螢幕，相關設定請參考「D-015 人員資通安全守則」。

4. 密碼應自行妥善保管，禁止貼在座位上。

5. 使用者每年應上資安教育時數 3 小時，建議自行上「e 等公務園+學習平臺」或「教師 e 學院」進行學習；考量部分同仁需求，圖書館亦將額外辦理實體教育訓練，如未取得線上時數者請務必參加。

6. 重要資料如個資，請勿外洩，如因業務需求傳送給其他人，請務必進行加密後提供(可以採 7zip 壓縮檔案設定密碼方式)，以免外洩需負法律責任，嚴禁未加密資料直接使用電子郵件或社交軟體如 line 傳送。

三、 核心系統向上集中辦理情形如下：

說明：

因學校依資安法規定應屬 C 級機關，惟 C 級機關應辦事項難以達成，故國教署提出核心系統向上集中規劃方案，計畫將學校 5 大核心系統移轉向上集中雲端化，以符合法規調降資安責任等級為 D 級，爰行政院核定學校端於 109 年底前資安責任等級暫列為 D 級，後續視向上集中情形調整。5 大核心系統移轉情形如下：

1. **校務系統**：國教署委由北科大開發公版程式，惟其系統尚不符學校需求，故尚未集中辦理。。

2. **學習歷程**：已由暨南大學完成向上集中。

3. **學校官網**：依規定自行完成中高風險弱點修補(高風險 46 個、中風險 39 個)，俟成大團隊通知辦理主機移轉事宜。

4. **電子信箱**：本校採用 G suite，依國教署建議行政人員應改採教育雲電子信箱使用，惟考量教師兼任行政交接情形不方便，且依教育部函示並未全面禁止，爰本校規範並未強制禁止使用，但考量資安等因素，仍要求各行政人員嚴禁使用電子信箱傳送含有個人資料信件，以免造成資安事件，如真有需要傳送敏感性資料，則請改用教育雲。

5. **DNS**：已完成向上集中至成大 DNS 管理系統。

四、　再次宣導請勿購買大陸品牌資通產品，如監視器、網路分享器、空拍機等，有網路功能者就不行，最近抓很嚴。

決議：洽悉。

捌、 討論及決議事項：

一、 有關本校資通安全政策修正一案，提請討論。

說明：建議刪除有關目標提到每年資安事件發生件數 4.2.1 及 4.2.2，並新增資安事件通報演練內容，詳如附件 1。

決議：無異議通過。

二、 有關今年度風險評鑑作業可接受風險值及風險評鑑結果，提請討論。

說明：

1. 風險值=資產價值(1~4)x 弱點(1~3)x 威脅(1~3)，建議調整可接受風險值為 12，超過 12 需進行風險改善作業，去年可接受風險值為 10。

2. 今年風險評鑑改善計畫如附件 2，風險值超過 12 以上計有不斷電系統設備老舊及電池過期，建議更換，因更換時需要斷電，故擬規劃於暑假期間辦理。

決議：無異議通過。

三、 有關本校今年度業務永續運作演練作業一案，提請討論。

說明：今年度擬演練項為模擬全球資訊網主機異常無法開機，由備份還原系統 Veeam 進行還原作業，並同步檢視備份資料之可用性，本次演練於 3/13 日上午演練完畢，演練結果成功，還原網站系統正常，資料內容正確，演練計畫如附件 3。

決議：無異議通過。

四、 有關 Google 雲端空間限制一案，提請討論。

說明：Google Workspace for Education 於 2022 年 7 月起限制學校教育端總使用容量上限為 100TB，故提請討論限制教職員及學生個別使用上限。初步建議個別限制如下，提請討論。

(一) 學生：1650 個，建議每人上限 50GB。

(二) 教職員：約 150 個，建議每人上限 200GB。

(三) 行政專用帳號：約 50 個，建議每人上限 500GB。

(四) 退休人員：暫時建議每人上限 50GB。如空間不足則不再提供使用。

(五) 實行起始日：110/09/01、111/03/01 或其他時間

備註：

1. 因與 Google 詢問後，表示於 110 年下半年才會提供管理端限制方法，故擬先暫時定期檢視，如超過容量擬先通知限期改善，未改善者先停權 1 周處罰，直至改善完畢。
2. 如空間不足建議可以改用微軟 Onedrive，學生皆有預先開設，教育版提供每人有 1TB 空間，教職員如有需求可以跟圖書館申請。

決議：從 110/08/01 開始施行，其餘無異議通過。

玖、 臨時動議

一、 有關資安健診所需經費說明

	資安健診項目	類型	所需人天	最低購買	金額
安全性檢測	網站安全弱點檢測	主機到場	0.35	15	4798
		主機遠端	0.3	10	
		WEB 到場	3	1	
		WEB 遠端	2	1	
		個資檢測	1	1	
	系統滲透測試	到場	16	1	5232
		遠端	15	1	
資通安全健診	網路架構檢視		2	1	4884
	網路惡意活動檢視	封包監聽分析	2	2	
		設備紀錄分析	1	2	
	使用者端電腦惡意活動檢視		0.3	20	
	伺服器主機惡意活動檢視		0.3	5	
	目錄伺服器設定檢視		0.5	1	
	防火牆連線設定檢視		0.5	1	

決議：洽悉。

壹拾、 附件

附件 1

1 目的

為確保國立彰化女子高級中學（以下簡稱本校）所屬之資訊資產的機密性、完整性與可用性，導入資訊安全管理系統，強化本校資訊安全管理，保護資訊資產免於遭受內、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 資通安全法(及施行細則)

2.2 個人資料保護法（及施行細則）

2.3 行政院及所屬各機關資訊安全管理要點

2.4 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、委外服務廠商與相關單等。

3.2 資訊安全管理範疇涵蓋 14 項領域，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本校造成各種可能之風險及危害，各領域分述如下：

3.2.1 資訊安全政策訂定與評估。

3.2.2 資訊安全組織。

3.2.3 人力資源安全。

3.2.4 資產管理。

3.2.5 存取控制。

3.2.6 密碼學(加密控制)。

3.2.7 實體及環境安全。

3.2.8 運作安全。

3.2.9 通訊安全。

3.2.10 系統獲取、開發及維護。

3.2.11 供應者關係。

3.2.12 資訊安全事故管理。

3.2.13 營運持續管理之資訊安全層面。

3.2.14 遵循性。

4 目標

維護本校資訊資產之機密性、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 確保相關資通安全措施或規範符合政策與現行法令的要求每二年至少進行一次內部稽核。

4.1.2 每二年至少進行一次資務持續計畫之測試或檢討。

4.2 定量目標：

~~4.2.1 確保資訊資產受惡意之侵襲，每年未經授權或因作業疏失對資產所造成的損害不得超過 1 件。~~

4.2.1 確保所有資通安全事件或可能之安全弱點，每年不依通報程序反應，並予以適當的調查及處理不得超過 1 件定期實施資通安全事件通報演練。

4.2.2 符合政府資通安全相關政策、規打及相關法令要求。

4.2.3 定期實施資通安全教育訓練。

4.3 本校完成指標時，需量下列項目：

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 本校應成立資訊安全組織統籌資訊安全事項推動。

5.2 管理階層應積極參與及支持資訊安全管理制度，並授權資訊安全組織遵循通過當的標準和程序以實施本政策。

5.3 本校全體人員、委外服務廠商與相關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，通報資訊安全事件或弱點。

5.5 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本校之相關規定進行懲處。

6 審查

本政策應每年至少審查乙次，以反映政府法令、技術及資務等最新發展現況及關注方之關注議題，以確保本校資訊安全管理制度之運作。

7 實施

本政策經「資通安全委員會」核定後實施，修訂時亦同。

風險改善計劃表					
文件編號	CHGSH-ISMS-D-013	機密等級	限閱	版次	1.0

紀錄編號：110-001　　填表日期：110 年 3 月 18 日

教育體系資通安全管理暨個人資料管理規範控制目標	現況說明	風險改善建議措施	教育體系資通安全管理規範條文	建議權責單位	預計改善時間與處理方式	與高風險資產之風險評估彙整表對照
實體及環境安全	EV001~EV005 不斷電系統設備老舊及電池年限過期	汰換已不敷使用之不斷電設備，並更新堪用設備之電池	A11.2	圖書館	預計 1100930 前完成更換	66~70

附件 2

附件 3

紀錄編號：110-001　　填表日期：110 年 3 月 13 日

演練規劃表		
承辦人：吳峻銘 協辦單位：圖書館 規劃日期：1100313		
演練規劃項目		規劃內容
1	規劃演練目標與範圍	全球資訊網
2	規劃演練腳本	全球資訊網無法正常開機，無法作業，故使用 Veeam 還原備份系統
3	規劃演練所需設備	無，系統已虛擬化
4	規劃演練所需系統	VMware 虛擬系統、Veeam 備份還原工具
5	規劃演練所需參與人員	吳峻銘
6	規劃演練時程及完成時限	03/13，預計 4 小時內完成
7	規劃演練測試方式與測試資源	確認系統是否開啟正常，產製報表(流通報表 1-4，3-2)確認
8	規劃演練成果的檢討時程	下次召開資安小組會議

演練暨處理執行表

承辦人：吳峻銘

協辦單位：圖書館

演練日期：1100313

演練開始時間	10：00	演練需要時間	2 小時
演練結束時間	12：00	實際作業時間	1 小時 20 分

演練執行項目		執行程序 （實際演練過程之執行紀錄）	負責人	執行結果
10:15	確認系統毀損，啟動 Veeam 備份工具還原昨日備份檔案	詳還原步驟流程	吳峻銘	成功
10:22	Veeam 還原系統	詳還原步驟流程	吳峻銘	成功
10:40	還原完成，開啟作業系統，確認系統是否正常	登入正常	吳峻銘	成功
11:00	修改網路啟動服務	網卡設定錯誤啟動失敗，修改網卡資料後啟動正常	吳峻銘	成功
11:20	確認網站正常公告資料到前一天	經比對一致	吳峻銘	成功
11:30	演練結束			

結果檢討：

本次演練確認備份資料正確無誤，且 Veeam 還原功能操作上極為便利，還原速度亦滿足本校需求。