彰化縣教育網路中心
所屬學校資通安全稽核綜合整理報告

稽核日期	**114年7月8日、114年7月9日、114年7月14日、114年7月24日、114年7月25日**

經綜整所屬學校資通安全實地稽核結果，說明稽核共通發現事項如下：

（一）策略面

1.1 學校應將資通安全政策公告於學校官網首頁以供內、外部利害關係人知悉。(2)

1.2 學校之管理審查會議之審查事項不符合ISO/IEC 27001及「資通安全維護計畫」之要求，其審查事項應應包括但不限於以下項目 (3)：

1.2.1先前管理審查決議事項之跟催狀況。

1.2.2與資訊安全管理系統有關之內部及外部議題的變更。

1.2.3與資訊安全管理系統有關的利害關係方的需求和期望的變化。

1.2.4資通安全的績效回饋，包含下列趨向：

1.2.4.1 不符合事項與矯正措施之執行狀況。

1.2.4.2 監督與量測結果。

1.2.4.3 內部稽核的結果。

1.2.4.4 資通安全目標的實現。

1.2.5資通安全維護計畫實施情形。

1.2.6利害相關團體的回饋。

1.2.7風險評鑑的結果與風險處理計畫的狀態。

1.2.8資通安全政策與目標適切性之審查。

1.2.9持續改進的機會。

1.3 學校未編列資安預算或所編列資訊安全相關經費不足，資安經費應依照行政院公布之「資安產業發展行動計畫」之規定，資訊經費中至少應編列7%之資安經費。(5)

（二）管理面

2.1 學校之資通系統與資訊資產納入同一清冊盤點，建議分別盤點，以利明確分辨資通系統及財產資訊。(6)

2.2 學校於進行資訊資產盤點時，雖已將資產納入資通系統資產清冊內，宜在資通系統資產清冊標註廠牌、型號等資訊，以利辨識是否為大陸廠牌。(6)

2.3 學校雖已依據資通安全維護計畫完成資通訊（產）相關之風險分析評估。惟未針對風險評估結果擬定因應控制措施，針對不可接受風險應擬定風險處理計畫，並進行殘餘風險再評估。(7)

2.4 學校與委外廠商之維護合約未將針對委外廠商之資安要求納入合約內容，如：不得為陸資、成員不得為陸籍人士、不得使用大陸廠牌資通設備、資安事件通報...等，不符合資通安全管理法施行細則第四條之要求。(24)

2.5 學校之一般人員與主管資通安全通識教育訓練未能滿足每人每年至少3小時之要求，依數位發展部之規定一般使用者及主管，除包含機關組織編制表內人員外，尚包含得接觸或使用機關資通系統或服務之各類人員。(25)

2.6 學校辦理內部稽核未針對不符合事項提出矯正預防措施，針對內部稽核之不符合事項應提出矯正與預防措施，並追蹤其改善成效，以符合ISO/IEC 27001 第十章之要求。(27)

（三）技術面

3.1 建議公用電腦加裝自動還原系統，以防止機敏資料遭到洩漏，並強化公用電腦之可用性。(9)

3.2 學校之個人電腦檢查未能落實執行，導致仍有以下常見不符合事項(11、12)：

1. 校內同仁未依規定時限變更密碼、密碼之長度及複雜度不符合要求，建議在沒有AD控管之下，可設定本機群組原則進行控管。
2. Windows 作業系統、防毒軟體及病毒碼未更新到最新版本，應保持更新至最新版本。
3. 自動播放功能未關閉。
4. 螢幕保護程式未開啟，或設定之時間超過15分鐘。
5. 個人電腦裝有遠端通訊軟體，如：ANYDESK、TEAMVIEWER。
6. 個人電腦安裝未經授權之軟體，如：WinRAR、嘸蝦米...等。

針對以上不符合事項請強化日常個人電腦之查核工作。

3.3 學校若機櫃放置於電腦教室內，屬半開放空間，且因機櫃無法上鎖，宜加裝監視器加以監控。(13)

3.4 學校之資訊機房應設置氣體式滅火器、緊急照明、UPS、冷氣等安全防護設備，並應維持在正常可用之狀態。(13、15)

3.5 學校之資訊機房平時已上鎖管理，但建議設置人員進出登記表並落實登記，以識別人員進出機房之時間。(14)

3.6 學校之資訊機房宜增設監控系統監視人員在內部之活動，以符合ISO/IEC 27001:2022條文A.7.4實體安全監控之要求。(15)

3.7 學校之非正式人員、臨時人員未簽訂保密切結書。(17)

3.8 資通安全維護計畫建議可再加入學校資安事件之通報窗口(如：本校之資通安全事件通報窗口及聯繫專線為：XX單位XX老師，分機1234)，以讓同仁知悉當發現資安事件時應向何人通報。(20)

3.9 學校對於所蒐集到的資安情資缺乏評估及採取因應措施之佐證紀錄，建議針對有採取行動之情資，應記錄其採取之行動進行紀錄以供佐證。(23)