臺中市立啟明學校資訊安全管理要點

105 年 6 月 24 日訂頒

106 年 2 月 20 日修正

壹、通則

一、依據行政院核定之「行政院及所屬各機關資訊安全管理要點」辦理。

二、為強化本校資訊安全管理，確保資料、系統、設備及網路安全，特訂定本要點。

三、要點以書面及電子方式公告本校教職員工及學生，並請提供資訊服務之廠商共同遵行。

四、本資訊安全管理要點實施後，需每年評估一次，以反映政府法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。

貳、組織及權責

一、本校有關資訊安全管理事務依下列分工原則：為統籌、協調、研議本校各項資訊安全之政策、計畫及資源調度，特成立「資訊安全管理小組」。

二、「資訊安全管理小組」設置資訊安全長（召集人）由校長兼任；資訊安全副組長由教務主任兼任；執行秘書為出版資訊組長兼任；並由秘書、各處室主任共同組成（如下表）；各處室主任及秘書為單位稽核人員。

臺中市立啟明學校資訊安全管理小組成員名單	
職務	職稱
資訊安全長兼召集人	校長
資訊安全副組長	教務主任

執行秘書	出版資訊組長
委員	秘書
委員	學務主任
委員	總務主任
委員	實輔主任
委員	人事主任
委員	會計主任

三、本小組各成員之任務如下:

（一）資訊安全長：

1.由校長擔任本小組之召集人，副組長協辦統籌資訊安全政策、計畫及技術規範之研議以及擬定或修正本校資訊安全政策。

2.督導及稽核資訊安全政策執行狀況及成效。

（二）執行秘書：

1.協助制定、執行及修正資訊安全政策。

2.決定單位內資安事件通報及應變處理事宜。

3.監督通報作業、應變計畫及資安演練之實施。

4.依據資安事件等級，授權系統復原作業之實施。

5.負責對內、對外之資訊安全聯繫事宜。

6.負責鑑定資安事件並依程序進行通報作業。

7.隨時掌握國家資通安全會報、臺中市政府教育局資訊教育暨網路中心或相關單位提供之資通安全危害通告資訊(如最新電腦病毒疫情、漏洞及駭客攻擊資訊等之預警訊息)。

8.發布資安訊息給校內所有人員，與系統管理人員保持連繫，並負責通告及監督系統漏洞修補與更新。

（三）稽核人員

1.協助單位每年實施內部稽核1次。

2.依據資安檢核表評估單位整體資安風險，提出改善建議事項。

3.協助資安事件之偵防演練作業。

四、本校每年進行一次資訊安全稽核。由秘書、各處室主任先做內部資安稽核（電腦安全自我檢查表)，發現問題記錄並反應至資訊安全小組協助處理。

參、人員管理及資訊安全教育訓練

一、本校依需要，辦理資訊安全教育訓練及宣導，建立員工資訊安全認知，提升學校資訊安全水準。

二、各單位負責重要資訊系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，實施人員輪調，建立人力備援制度。

三、資訊作業相關人員離職時，應取消其個人帳號和使用權限，並確實做好電腦軟硬體及相關文件之移交工作。

四、各單位業務主管應負責督導所屬員工之資訊作業安全，防範不法及不當行為。

五、資訊安全教育訓練及宣導事宜由資訊安全小組負責辦理。

肆、電腦系統安全管理

一、各單位辦理資訊業務委外作業時，應於事前研提資訊安全需求，明訂廠商之資訊安全責任及保密規定，並列入契約中，要求廠商遵守及定期考核，並派員監督。

二、電腦系統作業變更時，應詳實建立紀錄，以備查考。

三、各單位應依相關法規或契約規定，複製及使用軟體；嚴禁使用非法軟體。

四、電腦系統中應裝置防毒軟體並定期更新，磁片或隨身碟使用前應事先做掃毒檢查，以防止感染電腦病毒。

五、應遵守智慧財產權相關規定，使用者應遵守軟體授權規定，禁止使用未取得授權的軟體。

六、應依據電腦處理個人資料保護法等相關規定，審慎處理個人資訊。

伍、網路安全管理

一、各單位利用網路公佈及流通資訊時，應評估資料安全等級，機密、敏感性或未經當事人同意之個人隱私資料及文件，不得上網公佈。

二、本校非屬機密性或敏感性之資料及文件得以電子郵件或其他電子方式傳送。機密性或敏感性之資料及文件，欲利用電子郵件或其他電子方式傳送時，須以適當的加密或電子簽章等安全技術處理。

陸、系統存取控制

一、各單位對電腦資料庫及檔案應建立分級（機密及安全等級）管理制度。

二、各項正式作業之電腦系統操作及資料處理，由各權責單位指定專人負責建檔、核對、更新、審查及維護電腦資料之正確性。資訊系統發展人員非經核准不得操作使用或更改已正式作業之系統檔案。

三、電腦資料庫及檔案，應按不同業務範圍及使用權限，分別設定目錄、識別保護碼；重要或具機密性資料在建檔或提供使用時，應加設通行密碼、使用權限碼，以確保資料安全，且通行密碼應經常更新。

四、各單位離職、休職、調職人員，應立即取消使用單位內各項資源之所有權限和個人帳號，並列入人員離職、休職、調職之必要手續；人員職務調整及調動，應依系統存取授權規定，限期調整其權限。

五、各電腦系統應建立系統使用者註冊管理制度，建立使用人員名冊。

六、各單位之重要資料及系統委外廠商處理者，不論在機關內外執行，均應採取適當及足夠之安全管制措施，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

柒、系統發展及維護安全管理

一、各單位自行開發或委外發展之系統，應在系統之初始階段即將資訊安全需求納入考量；系統之維護、更新、上線執行及版本異動等作業，應予安全管制，避免不當軟體及電腦病毒危害系統安全。

二、對廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼；基於實際作業需要，得核發短期性及臨時性之系統辨識與通行密碼供廠商使用，但使用完畢後應立即取消其使用權限。

三、委託廠商建置及維護重要軟硬體設施時，應在本校相關人員監督及陪同下始得為之。

捌、資訊資產安全管理

一、各單位對於儲存各項機密資料或程式軟體之磁片、磁碟、磁帶、光碟片及報表等媒體，應設專人管理並定期備份，防止資料洩漏或損毀。

二、對於需要長期保留或重要檔案之備份資料，應存放在防火、防潮、防磁的設備中。

三、各業務單位需對使用之資訊資產進立安全管理，發現異常時應迅速通知服務廠商及本校資訊人員處理。

玖、實體及環境安全管理

一、各單位對於電腦設備之裝置地點，應考量使用及管理上之安全，並應指定專人負責管理，非經奉准之人員，不得隨意操作設備。管理或使用人員應詳細記載電腦設備故障、異常及維護等情形，以作為設備更新及作業安全 之依據。

二、電腦設備機房或電腦教室應設置適當之滅火設備。管理人員下班後，應關閉門窗及不必要之電源，以確保安全。

拾、業務永續運作之規劃

一、若發生資訊安全事件，應立即向相關人員通報，以採取適當反應措施。若有情節嚴重者，則聯繫檢警調單位協助偵查。

二、為因應各種人為及天然災害造成業務運作受影響，各業務單位需建立緊急應變及回復作業機制，並定期備份重要資料以及實體隔離。

拾壹、本要點經校務會議通過後實施，修正時亦同。