

【1140217 資安宣導各辦公室應辦理事項】

- 1.本校之資通系統（含公務電腦、辦公筆電）應設置通行碼管理，通行碼之要求需滿足：
 - (1)通行碼長度 8 碼以上。
 - (2)通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以上。(請勿使用弱密碼或帳號與密碼相同)
 - (3)使用者每 90 天應更換一次通行碼，應對個人所持有通行碼盡保密責任。
- 2.本校之主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。
- 3.校園電腦防毒軟體 100%啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
- 4.電腦、業務系統或自然人憑證，若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。
- 5.下班時應關閉電腦及螢幕電源。
- 6.筆記型電腦(行動設備)應安裝防毒軟體，並定期檢查作業系統修正程式與更新病毒碼為最新版本。
7. 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。

【所有人應辦理事項】

- 1.勿開啟來路不明或無法明確辨識寄件人之電子郵件。
- 2.禁止多人共用單一資通系統帳號。
- 3.知悉資安事件發生，能於規定的時間完成通報、應變及復原作業。
- 4.電子郵件社交工程演練之郵件開啟率及附件點閱率分別低於 5%及 2%。(請機關自行設定指標)
- 5.資安事件通報時間(含演練)超過一小時次數≤2 次。
- 6.校園電腦防毒軟體 100%啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
- 7.每人每年接受三小時以上之一般資通安全教育訓練。
- 8.本校依資通安全責任等級分級辦法之規定，屬資通安全責任等級 D 級
- 9.本校之資通系統應設置通行碼管理，通行碼之要求需滿足：
 - (1)通行碼長度 8 碼以上。
 - (2)通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以上。(請勿使用弱密碼或帳號與密碼相同)
 - (3)使用者每 90 天應更換一次通行碼，應對個人所持有通行碼盡保密責任。
- 10.本校之主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。

- 11.本校配合向上集中計畫，校內無電子郵件伺服器，校內同仁均申請教育部校園雲端電子郵件為公務信箱。
- 12.本校人員到職後應經申請方可使用電子郵件帳號，並應於人員離職後刪除電子郵件帳號之使用。
- 13.電腦、業務系統或自然人憑證，若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。
- 14.禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。
- 15.連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
- 16.筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
- 17.下班時應關閉電腦及螢幕電源。
- 18.筆記型電腦(行動設備)應安裝防毒軟體，並定期檢查作業系統修正程式與更新病毒碼為最新版本。
- 19.禁止使用危害國家資通安全產品與大陸廠牌資通訊產品(含軟體、硬體及服務)