電子計算機中心通知

依據教育部 110 年 6 月 29 日臺教資(四)字第 1100085899 號來文，針對教育部所屬大專校院，爾後如有因管理不當導致資安事件，將以不遮蔽校名方式作為教育體系內部案例宣導，另將專案實地稽核，未落實稽核缺失改善者，將循相關機制提報懲處。

惠請各系所單位周知所屬教職員工生，執行公務務必留意資訊安全及個人資料保護原則，避免觸法並維護校譽。

資訊安全宣導事項

- 處理公務應使用機關提供之資訊設備、網路，及規定之軟體，勿任意安裝不明軟體、連結不明網站或開啟不明電子郵件，以免感染電腦病毒、木馬或惡意程式。
- 作業系統應經常更新，修補程式漏洞，避免被駭客攻擊(例如：勒索病毒)。
- 一般使用者及主管，每年應接受 3 小時以上之資通安全通識教育訓練，以維持並強化個人對資通安全的新知新見。
- 個人電腦應安裝掃毒軟體，定期更新病毒碼，防堵可能中毒的網路管道，隨身碟或外接式硬碟等儲存設備，放入電腦讀取前應先進行掃毒再使用。
- 公務用之資通訊產品不得使用大陸廠牌，且不得安裝非公務用軟體。
- 公務資料應定期備份，可以在中毒或遭受攻擊時將損失風險降到最低。
- 不使用公務電子信箱帳號登記做為非公務網站的帳號，如社群網站、電商服務等。
- 公務資料傳遞及聯繫應使用公務電子郵件帳號，不使用非公務電子郵件傳送或討論公務訊息。
- 應注意不使用即時通訊軟體傳送帳號、密碼或公務敏感資料。
- 傳送公務資訊或個人資料等，應有適當保護，例如加密傳送。
- 帳號密碼必須妥善保存，並遵守機關規定，密碼設定應注重複雜度，禁止使用與帳號名稱相同、身分證字號、學校代碼、易猜測之弱密碼或其他公開資訊，如有外洩疑慮，除了儘速更換密碼

外，應通報資安窗口。特別是主管等級密碼，務必留意安全設定，避免電子郵件被盜用，成為單位詐騙工具。

- 業務承辦人接獲指示交辦之郵件，應小心求證，確認為長官或業務相關對口之本意，方可配合辦理。
- 委外辦理資通系統時，應將資通系統依防護基準要求之安全需求，明定委外契約，並於上線前落實安全檢測。
- 資通系統存取控制，應採最小權限原則，非業務需要，不得提供授權。
- 有資安疑慮或異常時，應即時通報資安窗口。
- 應遵守個人資料保護法及資通安全管理法之相關要求。

個人資料保護宣導事項：

- 各單位(包含行政單位、教學單位、學生社團)處理教職員工生之個人資料時，應依據「個人資料保護法」及相關規定處理，不可違反個資法，蒐集、洩漏個資或進行非公務以外之用途。
- 遇有學校以外單位索取個資時，主管單位應依據「個人資料保護法」及相關規定嚴予審查，並簽奉校長核可方能提供資料。
- 個人資料之傳遞，應採安全可靠之機制，如以電子檔傳送，應對資料檔案壓縮加密後方可傳輸；如以實體文件(紙本)傳遞，應裝袋並彌封，所有傳遞行為應加以記錄流向備查。
- 業務承辦人所持有之個人資料檔案應加密保護，使用完畢後，應立即退出應用程式。
- 承辦各項活動時，應採用最少個資方式陳列，勿將不相關之敏感個資(如身分證號、出生日期、電話...)公開於活動資料、海報或簽到簿。
- 為行政目的使用資通系統或雲端資通服務(如 Google 表單、Microsoft Forms 等問卷調查服務)涉及蒐集個人資料者，應注意資料蒐集是否最小化，也要留意各項存取控制及詳閱設定內容，以維護個人資料之安全性。
- 資訊設備應設有螢幕保護程式，並設定密碼，承辦人離開座位時應啟動螢幕保護。
- 各項密碼至少每三個月應更換一次，應注重提升密碼之長度及複雜度，以有效保護個人資料。
- 禁止使用各項即時通訊軟體(如 LINE、SKYPE、WECHAT...)傳遞個資。

- 處理個資檔案之資訊設備如需報廢或移轉他用時，應確實銷毀設備內之個人資料檔案。
- 應遵守個人資料保護法及資通安全管理法之相關要求。

請參考本校資安及個資保護專區：
https://www.ncyu.edu.tw/pims/index.aspx

本校 ISMS+PIMS 文件專區(限校內瀏覽): http://10.17.200.80/

此致

本校各單位院系所

電子計算機中心 敬啟