教育體系電子郵件服務與安全管理指引

一、教育部（以下簡稱本部）為確保各級學校、臺灣學術網路區域網路中心、各直轄市、縣（市）教育網路中心電子郵件服務安全使用，減少不當使用及降低資通安全威脅，特訂定教育體系電子郵件服務與安全管理指引（以下簡稱本指引）。

二、本指引適用對象為各級學校、臺灣學術網路區域網路中心、各直轄市、縣（市）教育網路中心（以下簡稱各單位）。

三、各單位辦理公務業務或核心業務時，應使用單位配發之電子信箱收發公務所需資訊，不得使用非公務信箱進行公務郵件收發等事宜。

四、各單位建立電子郵件服務時，應明確規範電子郵件服務對象（教職員、學生、校友、校外人士、電子郵件服務人員及廠商、資安人員）、申請方式、使用用途範圍及使用期限，且不得提供服務對象以外者使用電子郵件服務。

各單位建立前項電子郵件服務，應訂定電子郵件服務使用相關規範，明確規範使用者之權利、責任及相關安全原則如下：

（一）初次申請者應驗證使用者身份。

（二）應強制使用者最低密碼複雜度；強制密碼最短及最長之效期。

（三）使用者使用電子郵件服務時，不得散布詐欺、誹謗、侮辱、猥褻、騷擾、非法軟體交易或其他違法之訊息，導致他人權益受損。

（四）使用者使用電子郵件服務時應尊重智慧財產權，不得有違法傳送或侵害他人智慧財產權之行為。

（五）使用者使用電子郵件服務時不可作為商業用途。

（六）使用者使用電子郵件服務時，應尊重網路隱私權，不得任意窺視其他使用者之個人資料或有其他侵犯隱私權之行為。不得盜用他人或系統資源，或以任何方式影響系統正常運作。

（七）使用者辦理公務、及重要（或敏感）專案使用之電子郵件信箱（可規劃專用電子郵件信箱），不得轉至外部私人信箱收發公務資訊。

（八）教職員如轉任或借調至公務機關服務者，不得使用學校電子郵件信箱收發公務機關相關電子郵件。

（九）使用者如因故無法使用公務信箱讀取訊息，以致影響公務執行，得由直屬單位主管指定代理人提出申請，並經郵件維護負責單位審核必要性後，授權代理人讀取公務信箱相關內容。

各單位訂定之前項規範，應辦理教育訓練，以利使用者了解並落實遵守相關規範。

五、各單位委外辦理電子郵件服務系統建置，應考量受委託者之專業能力與經驗，選任適當之受託者，監督其資通安全維護情形，並注意資通安全管理法施行細則第四條第一項各款事項。

各單位應提供適當之加密或認證相關機制（或工具），作為公務郵件傳送敏感性資訊時採用。

前項傳送敏感性資訊時，應採用傳輸層安全性協定（Transport Layer Security）傳輸。

六、各級學校應將應用於學校校務行政及教學等重要業務之電子郵件服務納入核心資通系統，辦理業務持續運作演練及網站安全弱點檢測，並導入資訊安全管理系統，大專校院應通過第三方驗證。

各單位視資源能力設置適當之安全防護系統及設備，並應注意資通安全管理法相關規定。

各單位應備電子郵件過濾機制，視資源能力對電子郵件特徵（來源網域名稱、IP、電子郵件地址，發信量、發信次數等）實施必要檢查，以強化電子郵件服務安全。

七、各單位自行開發或委外開發建置電子郵件服務系統，應辦理資通安全責任等級分級作業辦法附表十資通系統防護基準至少「中」以上之控制措施。

各級學校內部單位如有建置電子郵件服務系統，應向學校網路管理部門提出服務架設申請，以利學校垃圾郵件統一管控。

八、各級學校接受政府機關（構）委託辦理具有國家安全機密性或敏感性業務或技術研究者，應使用通過第三方驗證之電子郵件伺服器及信箱，且該信箱不得作為非公務之個人信件收發使用。

前項之電子郵件伺服器應強化安全性檢測及防護基準如下：

（一）每半年辦理一次網站安全弱點檢測並完成弱點修補。

（二）落實資通安全責任等級分級作業辦法附表十資通系統防護基準有關「系統與通訊保護」構面之「高」等級控制措施。

九、各單位應定期辦理使用電子郵件服務教育訓練，提醒使用者勿開啟來路不明之電子郵件，並加強如電子郵件相關政策、管理、使用注意事項及新型態威脅等資安宣導。

各單位應配合本部每年定期辦理防範惡意電子郵件社交工程之演練作業，進行單位人員教育訓練，並勿過濾測試郵件，以加強使用者之安全警覺意識。

各單位應針對前項演練不合格人員加強資安訓練及宣導。

十、各單位應持續監控電子郵件服務效能及通信紀錄，並保存相關軌跡，遇大量異常郵件、異常設定自動轉寄、異常權限變更等異常情形時，應依臺灣學術網路各級學校資通安全通報應變作業程序規定，即時至臺灣學術網路危機處理中心（TACERT）通報資安事件，啟動緊急應變作為（區域網路中心及直轄市、縣（市）教育網路中心適時提供必要協助），分析遭攻擊情況、攻擊管道，採取必要之損害管控及防護措施。

十一、各單位電子郵件服務提供與使用，本指引未規定者，依資通安全管理法及本部相關資通安全規定辦理。