國立屏東科技大學資通安全管理政策

113.01.31

一、國立屏東科技大學(以下簡稱本校)為強化資通安全管理、增進本校及電子計算機中心同仁對資通安全之認知，並確保資通安全管理、資料、系統、設備與網路安全，特訂定本政策。

二、為統籌資通安全管理等事項之協調及推動，成立資通安全管理小組，該小組之幕僚作業由電子計算機中心負責。

三、依下列分工原則，配賦有關單位及人員權責：

（一）資通安全管理政策、計畫及規範之研議、建置及評估等事項，由電子計算機中心負責辦理。

（二）資料及資訊系統之安全需求研議、管理及保護等事項，由本校各業務單位負責辦理。

（三）資通訊保密維護及安全稽核等事項，由電子計算機中心會同相關單位負責辦理。

四、本政策之範圍如下，有關單位及人員應就下列事項訂定相關管理規範及資通安全目標，並定期評估實施成效：

（一）資通安全政策適用性。

（二）資通安全暨利害關係人管理。

（三）存取控制管理。

（四）供應商管理。

（五）資通安全事件通報管理。

（六）營運持續管理。

（七）法規遵循性管理。

（八）人力資源管理。

（九）實體及環境安全管理。

（十）網路安全管理。

（十一）資料備份管理。

（十二）密碼控制管理。

（十三）資通系統及資訊資產管理

（十四）系統發展及維護安全管理

（十五）資通安全稽核管理

五、本校政策至少每年會在管理審查會議中檢討一次適切性，以反映法令、技術及業務等最新發展現況，確保資通安全實務作業之有效性。

六、本校資通安全管理小組暨利害關係人管理：

（一）資通安全管理小組由行政副校長擔任資安長，電子計算機中心主任為執行秘書、置委員若干人，透過小組的運作，來強化資通安全管理的橫向連結與溝通，進而優化本校資通安全管理的能力。

（二）本校利害關係人包含學生、學校職員、學校老師、本校同仁、軟/硬體廠商、主管機關，每年透過本校同仁與利害關係人互動狀況，來評估需求，進而協助本校的資通安全管理，可以更符合利害關係人的期望。

七、存取控制管理

（一）系統存取應依人員職務或角色，訂定相關權限。

（二）離(調)職人員，應立即取消各項資訊資源之所有權限，並列入離(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。

（三）建立系統使用者註冊管理制度，加強使用者通行密碼管理，使用者通行密碼之更新周期，最長以不超過六個月為原則。

（四）對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，課其相關安全保密責任。

（五）建立資通安全稽核制度，定期或不定期進行資通安全稽核作業。

（六）讓資訊刪除、資料遮蔽、資料洩露預防、儲存紀錄、特殊權限公用程式之使用得到有效管理。

八、供應商管理

（一）透過採購流程評選後，可採用之供應商，會簽署合約或保密協議，才能進行本校資訊軟體及硬體的服務。

（二）供應商服務人員的異動，也應通知本校知悉，經本校同意後，才可進行資訊服務作業。

（三）供應商維修服務的門禁及系統權限管理，均應遵守本校規定。

（四）建立 ICT 供應鏈中之資通安全管理。

九、資通安全事件通報管理

（一）各項資通安全活動或服務過程之意外與緊急事故鑑定。

（二）資通安全緊急事故通報。

（三）建立資通安全事件緊急處理機制，在發生資通安全事件時，應依規定之處理程序，立即向資訊單位或人員通報，採取反應措施，必要時，並聯繫檢警調單位協助偵查。

（三）資通安全意外與緊急事故應變之測試與訓練。

（四）持續監控、管理及改善資通安全。

十、營運持續管理

（一）依風險評估高風險項目、營運衝擊分析、資通安全策略、日常營運持續需求或資通安全事故等持續營運需求來源，訂定營運持續運作計畫。

（二）營運持續包含資通安全政策、處理流程、處理人員及 ICT 架構。

（三）針對營運持續 ICT 架構訂定緊急應變、回復作業程序及降低營運持續風險計畫。

（四）並定期演練及調整更新營運持續計畫，讓營運持續從困難中迅速恢復的能力提升。

十一、法規遵循性管理

（一）每年應定期蒐集資通安全相關法規。

（二）與本校有關資通安全相關法規應上網公告。

（三）強化對智慧財產權、隱私及個人識別資訊 PII 保護。

（四）針對不符合資通安全法規條款，應通知相關同仁處理。

十二、人力資源管理

（一）對資訊相關職務及工作，應進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，並進行必要的考核。

（二）針對管理、業務及資訊等不同工作類別之需求，定期辦理資通安全教育訓練及宣導，建立同仁資通安全認知，提升資通安全水準。

（三）建立適切的資通安全獎懲措施。

十三、實體及環境安全管理

（一）須採取適當的門禁管制，以防止對資通資產不當存取或造成損害，對外提供服務之主機系統與網路設備及對內服務之網路伺服器均須放置於有適切門禁管制之場所。

（二）進入辦公場域或管制區域，非本校之人員，須由本校人員在場陪同下，方可進入本校工作區域。

（三）本校所有人員須遵守電腦螢幕保護及桌面淨空原則，存放機密資料之抽屜及櫥櫃之保管人在離開辦公場所時須將其上鎖。

（四）實體安全監視、場所外資產之安全、儲存媒體、支援之公用服務、佈纜安全、設備維護、設備汰除或重新使用之保全，都在可控的作業環境下運作。

十四、網路安全管理

（一）架設硬體防火牆、入侵偵測系統及弱點掃描等，來阻隔來自網際網路未知的入侵攻擊，以保護網站資料的安全及完整性。

（二）安裝網路監控系統，監控網路流量，針對異常之狀況，發揮即時控管的功效。

（三）架設防毒系統，以防止病毒之入侵，提供使用者一個安全的網路環境。

（四）定期與不定期備份網站資料，當不可預期的災害發生後，以期能在最短時間內使系統復原，繼續上線服務廣大的使用者。

（五）定期或不定期更新相關作業系統或應用程式廠商所發布的相關更新程式，以確保系統對於任何攻擊的防禦性，使遭受攻擊的機率降到最低。

（六）確保使用雲端服務之資通安全及啟動有限的遠端連線功能，減少資通安全風險。

十五、資料備份管理

（一）應針對重要資訊與軟體進行定期備份作業，以便在發生系統失效或資料錯誤時，可迅速地回復正常作業，及還原正確資料。

（二）各項系統設定檔、伺服器檔案及資料庫資料均應由各系統負責人員訂定備份週期。

（三）備份管理人員應注意備份系統運作是否正常，並不定期抽查系統之鐘訊同步狀態與運作紀錄。

十六、密碼控制管理

（一）透過帳號及密碼管理複雜度及長度的管制，再配合系統存取權限控制，來有效管理校整體系統密碼。

（二）同仁應定期變更密碼，以避免密碼被不當使用。

十七、資通系統及資訊資產管理

（一）建立與資通系統有關的資通資產目錄，訂定資通資產的項目、擁有者及資通資產分類等。

（二）已列入資通資產安全分類的資通及系統之輸出資料，應標示適當的保密等級以利使用者遵循。

（三）核心系統所延伸的 ICT 設備，進行資通處理設施之多備源鑑別。

十八、系統發展及維護安全管理

（一）自行開發或委外發展系統，應在系統生命週期之初始階段，即將資通安全需求納入考量；系統之安全程式設計、維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、後門及電腦病毒等危害系統安全。

（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。如基於實際作業需要，得核發短期性及臨時性之系統辨識及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之軟硬體設施，應在本校相關人員監督及陪同。

十九、資通安全稽核管理

（一）建立全校性年度稽核計畫以符合 ISMS 與相關法令或法規之要求。

（二）訓練合格稽核員，建立稽核查檢表格，執行稽核作業。

（三）進行稽核檢討與改善，持續資通安全管理有效性。

二十、本資通安全管理政策由資安長核可後實施，修正時亦同。