中臺科技大學資訊設備安全管理作業規範

文件編號：CAR115
1040722 行政會議通過
1070905 行政會議修訂通過
1100825 行政會議修訂通過更改單位或主管名稱
1120308 行政會議修訂通過

一、為加強督促改善校內之資訊安全防護，避免因人為疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或破壞等風險，而影響電腦系統正常運轉，制定「資訊設備安全管理作業規範」（以下簡稱本規範）。

二、適用範圍

（一）人員：

中臺科技大學（以下簡稱本校）之教職員工（含約聘僱人員及計畫助理）、學生等使用本校資訊資源，或資訊業務委外服務之廠商人員。

（二）資訊設備：

1.硬體設備：指個人電腦、工作站、主機、伺服器、筆記型電腦、顯示器、可攜式資訊設備及儲存媒體、印表機（含連接線材）及其他電子週邊設備。

2.軟體設備：指安裝於電腦內部供執行使用之程式（含系統軟體、套裝軟體、應用軟體及資料）。

三、管理及權責

(一) 圖書資訊處（以下簡稱本處）為本校資訊設備安全管理之督導單位。

(二) 各單位為業務用資訊設備之使用單位，所屬之資訊設備應有保管人並依據本校「財物管理辦法」規定負責單位內資訊設備之安全管理事宜。

四、人員安全管理與資訊安全教育訓練

(一) 各單位主管應負責督導所屬教職員工之資訊作業安全，防範不法及不當行為。本校教職員工（含約聘僱人員及計畫助理）、學生等，校內人員須簽署「資訊安全保密切結書」，確實遵守本校規範。

(二) 本校資訊業務，若有委外服務之廠商，應於簽訂契約時，校外廠商人員須簽署「資訊安全保密協議書」，確實遵守本校規範。

(三) 本校人員須參與本處主辦的資訊安全教育訓練及宣導，建立並加強資訊安全認知，提升資訊安全水準。

(四) 各單位重要系統之管理、維護、設計及操作，應建立人力備援機制。

(五) 如因職務異動成為非授權使用者時，隸屬單位應主動通知各單位更改使用者密碼或刪除該使用者帳號。

(六) 各單位人員離職時，須依規定辦理離職手續，並終止相關資源之存取權限，確實做好電腦軟硬體及相關文件之移交工作。

(七) 違反本規範者，將依本校相關獎懲辦法查處。

五、資訊系統安全管理

(一) 資料庫或個人重要資料應定時執行備份，並異地存放，以確保資料的安全。

(二) 處理含個人資料時，應依據「個人資料保護法」及相關規定審慎處理。

(三) 各單位之個人資料索取或調閱，須經單位主管核准，依據「個人資料保護法」及相

關規定審查後，始可提供資料。

(四) 應使用合法版權軟體，避免使用來路不明軟體。

(五) 與外部交換機密敏感資料時，需依據安全查核機制，確定無安全疑慮，方可進行。

(六) 需安裝防毒軟體，隨時更新病毒碼，並定期下載系統漏洞修補程式。

六、系統存取控制

(一) 賦予使用者適當的系統存取權限。但工作調整時，適當調整系統存取權限。

(二) 使用者不可多人使用同一組帳號密碼。密碼必須加以保密，避免洩密遭人盜用，並應定期更改密碼。

(三) 人員因故離開座位暫停作業時，必須登出系統或使用畫面鎖定保護。

七、資訊資產之安全管理

(一) 建立資訊系統有關資訊資產目錄，明列資訊資產的項目、管理人，如有變更應詳細記載。

(二) 資訊設備故障，應由管理人負責處理。

(三) 資訊資產報廢應依本校「財物管理辦法」規定辦理。

(四) 儲存媒體應在報廢處理前詳加檢查，予以實體銷毀。

八、設有伺服器之單位實體及環境安全管理

(一) 資訊設備安全管理

1.專人負責，並制訂資訊設備開關機操作程序。

2.應定期維護保養。

3.資訊設備、資料或軟體，未經管理人員同意下，不得攜離辦公區。

4.資訊傳送過程，應有妥善的安全措施，以防止資料遭竄改、破壞、誤用或未經授權的取用。

(二) 電力供應系統的管理

1.各單位於新增硬體設備時，應先評估電力負載。

2.相關資訊設備之電源使用，應依據製造廠商提供規格設置。

3.緊急供電系統暨不斷電系統（UPS System），應由專人負責管理及制訂開關機操作程序，並定期維護保養及測試。

(三) 電腦機房消防系統的設置及管理

1.應設置滅火設備及專人負責管理。

2.應定期維護環境安全、設備保養及測試。

(四) 其他安全管理

1.電腦機房應實施門禁安全控管，進出機房應填寫「進出機房記錄簿」。

2.資訊支援或維護服務人員，需由管理人員陪同並經登記後，始得進出管制區域。

3.電腦機房及各項軟、硬體設備，應加裝攝影設備強化防護措施。

4.列印之各式報表、作業程序目錄、及系統文件等保密資料應納入管理。

九、本規範經行政會議通過後實施，修正時亦同。