德明財經科技大學

實體環境安全管理規定

機密等級：一般

文件編號：Takming-ISMS-B-006

版　次：V 1.3

初版日期：107.12.25

修 訂 紀 錄

版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	107.12.25	N/A	執行小組	初版
1.1	108.09.11	1，5	執行小組	增加”廠商”二字
1.2	114.02.07		推動小組	”本中心”改”本校”
1.3	115.06.08	5	推動小組	新增場所外設備安全事項

1 目的

確保德明財經科技大學(以下簡稱本校)辦公室與電腦機房之安全管理，有效運用各項資訊設備，以確保相關資訊系統正常維運。

2 適用範圍

本校辦公室與電腦機房環境內之設備、內部人員、外部人員均適用之。

3 名詞定義

3.1 辦公區域

泛指本校除電腦主機房區域外之辦公作業環境。

3.2 電腦主機房區域

泛指本校電腦主機房區域。

3.3 內部人員

指本校之專兼任教職員工、約聘僱人員等。

3.4 外部人員

除本校人員外，短時間(臨時)於辦公區域活動之人員(如:廠商，訪客等)。

4 權責

4.1 機房門禁系統管理人員

負責機房門禁權責授予、控管(製作表單控管)機房門禁卡發放等作業。

4.2 電腦機房維運人員

4.2.1定時巡視電腦機房，確保電腦機房機電設備、空調、保全、監視系統及消防設備之安全管理與正常維運。

4.2.2如遇資訊安全事件，依據「資訊安全事件通報管理規定」辦理。

4.3 系統操作人員

4.3.1廠商進出電腦機房須記錄於「電腦機房廠商進出管制登記表」。

4.3.2確保本身負責之資訊設備正常運作。

4.3.3廠商維護時須陪同。

4.4 權責主管

4.4.1負責核准相關設備使用，並督導電腦機房設備之安全管理。

4.4.2檢視電腦機房進出登記紀錄。

5 要求事項

5.1 實體安全周界

5.1.1應明確區分辦公區域、電腦機房、會議室、電腦教室、機電室等實體安全周界。

5.2 實體進入控制

5.2.1為確保設備及資料之安全，應採用有身分識別功能之安全門，

做為必要之安全控管。

5.2.2重要之出入口均應設置門禁管理及錄影監視系統。

5.2.3內部人員於進出時應隨時注意是否有非經授權人員跟隨進入。

5.2.4機房門禁卡申請與管理

5.2.4.1 申請者依據本身業務之需求，向機房門禁系統管理者提出申請，並填寫「電腦機房門禁卡使用登記表」。

5.2.4.2 人員離、調職時，若該員有進出機房之權限時，待依人事相關法規辦理後由機房門禁系統管理人員註銷其門禁權限。

5.2.5本校非管理人員進出本校電算中心機房時，應配帶教職員證或識別證(工作證)。

5.2.6外部人員或委外人員應配帶原公司所製發之員工證或相關證明，並應於指定環境內執行作業。

5.2.7除機房管理人員外，其他因業務需要進入電腦機房作業時，應由機房管理人員陪同進入。

5.2.8機房出入口及機房內應設 24 小時動態監控，錄影紀錄應至少可前溯 15 天。

5.2.9門禁系統之進出紀錄應定期備份；紀錄存放於安全區域並保存半年備查。

5.3 保全之辦公室、房間及設施

5.3.1進入辦公室環境或機房，未經許可禁止使用錄音、錄影照相設備及可攜式資訊存取設備。

5.3.2資訊資產之使用及管理，依據「資訊資產管理規定」辦理。

5.3.3個人電腦、伺服器應設定螢幕密碼保護程式，螢幕保護程式啟動時間設定不應超過 10 分鐘。下班時應關閉不需使用之個人電腦。

5.3.4應實施桌面淨空，重要文件應妥善保管。

5.3.5使用影印機、印表機、傳真機或多功能事務機後，應立即將資料取走。

5.4 交付及裝卸區

5.4.1辦公區域或電腦主機房應設置物品卸載區，於大型設備報廢或新購時，搬運裝載相關物品使用。

5.4.2應由專人負責處理公文、郵件之收發。

5.5 電腦機房環境安全管理

5.5.1重要設備如大型主機、伺服器等，應置於電腦主機房。

5.5.2內部人員、外部人員於辦公區域或電腦機房使用非本校之資訊設備、可攜式設備時，依據「資訊資產管理規定」辦理。

5.5.3電腦機房內應保持整齊清潔，並嚴禁攜帶飲料及食品進入。

5.5.4電腦機房內禁止吸煙及飲食。

5.5.5電腦機房內禁止堆置易燃物(例如紙箱等)。

5.5.6電腦機房應設置安全出入口，並有明顯逃生路線標示。

5.5.7電腦機房內應設置停電緊急照明設備。

5.6 防範外部及環境威脅

5.6.1電腦機房應設置專用之消防器材或系統，如火災警報、滅火設備等，同時應符合相關法規並定期檢測、記錄。

5.6.2電腦機房內實體環境應考量耐震、防火、防水、防盜及可監控之設計。

5.6.3各式人為或天然災害如設備電源中斷、設備故障、水電空調故障、火災、水災、地震、颱風等緊急狀況，依據「資訊安全營運持續管理規定」辦理。

5.6.4電腦機房溫濕度採固定區間控制，溫度應維持在 18℃ 至 28℃，相對溼度維持在 30%至 70%。

5.7 支援的公用設施

5.7.1應保護設備免於電源失效，及因其他支援之公用服務事業失效，所導致之中斷。

5.7.2電腦機房應設置不斷電設備及發電機，以保障正常維運。

5.8 佈纜安全

5.8.1實施蟲、鼠害等防治措施，以保護線路及相關設備。

5.8.2電腦機房高架地板應考量重量承載能力(500kg/m)、耐震功能。

5.8.3電腦機房設備、主機、線路等應有適當標示，且排列放置定位，便於突發狀況時迅速處理與日常管理。

5.8.4網路通訊設備於安裝時，應注意機房之電力線路架構，以避免產生線路間之干擾問題。

5.8.5光纖或是易遭受破壞之線路設施應妥善保護，以免因其他工程裝設而影響網路之運作。

5.8.6線路採用天花板高架或佈建於高架地板下，以防止線路遭破壞或損毀。

5.9 設備維護

5.9.1電腦機房維運設備

5.9.1.1 電腦機房維運人員應隨時注意電腦機房相關設施是否有異常現象，如發生異常，應即時處理並通知相關人員或權責主管、相關單位或廠商；並將檢查處理情形記載於「異常事件紀錄表」。

5.9.1.2 電腦機房維運設備(如消防、電力、空調設備等)或重要資訊設備(如主機、網路設備等)應與合格專業廠商簽訂維護合約，定期實施保養與妥善維護，以確保設備的完整與安全。

5.9.1.3 外部廠商作業完成後，需提供維護處理紀錄表單，以備

查詢。

5.9.2資訊設備維護要求

5.9.2.1 資訊設備應視實際需求簽訂維護合約，以維護設備可用性及完整性。

5.9.2.2 如牽涉機密性資料之相關委外維護工作，依據「資訊作業委外安全管理規定」辦理，要求廠商填寫「委外廠商保密切結書」並與廠商簽訂安全條款。

5.9.2.3 廠商進入本校電算中心執行設備安裝維護作業時，應獲得資訊設備負責人員授權，必要時由資訊設備負責人員陪同與監督，並依據不同設備，要求廠商提供維護紀錄副本或填寫維護紀錄，由該員妥善保管。

5.9.3資訊設備維修考量

5.9.3.1 資訊設備送修時，若非屬儲存媒體損壞，於送修前應先取出儲存媒體，不得一起送修。

5.9.3.2 儲存媒體送修時，若內含機密性資訊時，應先進行備份，存放於安全區域，並徹底刪除送修設備上之機密資訊，防止資訊外洩。

5.9.3.3 報修外送應經由權責單位主管核准。

5.9.3.4 合約規範之外修作業，修復後發現資訊設備規格不符，則依合約規範處理。

5.9.4報修及維修程序

5.9.4.1 個人電腦、終端印表機等終端設備

辦公室資訊設備、個人電腦維修作業，依據本校維修流程進行維修。

5.9.4.2 主機端系統(含伺服器、主機、網路設備等)

(1) 於上班時間，使用者、應用系統負責人或同仁發現系統發生異常事故，逕行通報相關負責人；於非上班時間，使用者發現系統發生異常事故，逕行通報值班人員並由其電洽系統負責人或其權責主管。

(2) 設備異常時，由設備系統負責人進行初步研判或處理，能自行解決於確認後結案，若影響應用系統之運作，應通知應用系統負責人。

(3) 系統負責人或其權責主管接獲設備異常通報，則依據「資訊安全事件通報管理規定」辦理。

(4) 系統發生異常若須報請設備維護廠商進行維修，系統負責人得自行報修。

(5) 上班時間廠商維修由系統負責人進行監督；非上班時間由值班人員進行監督並得視個案需要電話通知系統負責人或其權責主管。

5.10 財產進出管制

5.10.1 攜出入機房內之資訊設備(含可攜式資訊設備/媒體)皆應遵守下列規定：

5.10.1.1 外部人員進出機房，須填寫「電腦機房廠商進出管制登記表」，若有攜入設備時，系統操作人員負責掃毒確認安全。

5.10.1.2 資訊設備之異動須經權責主管核准後方得異動；如須攜出或攜入資訊設備請填寫「設備進出紀錄表」。

5.10.1.3 廠商借測設備進入電腦機房，非經授權不得與本校網路連線，因設備借測所導致之洩密損失賠償及刑事責任，概由廠商負責，並列入本校拒絕往來戶。

5.11 場所外設備安全宜考慮事項

5.11.1 攜出場所外之設備和媒體，應對硬碟或 USB 先進行加密措施，留置在公共場所時不宜無人看管；外出洽公時，宜將手提電腦當作手提行李攜帶，並儘可能加以偽裝。

5.11.2 攜出場所外之設備，欲進行遠端存取時，必須透過 VPN 連線。

5.11.3 攜出場所外之設備和媒體若不慎遺失或遭竊，需第一時間進行通報。

5.12 無人看管的使用者設備

5.12.1 個人電腦限制執行資源分享，必要時應由權責主管同意，並設定密碼保護。

5.12.2 使用者離開電腦設備時，應退出使用環境或電腦螢幕鎖定，以確保資料之安全。

5.12.3 個人電腦、伺服器或主機應設定螢幕密碼保護程式，螢幕保護程式啟動時間設定不應超過 10 分鐘。

5.13 桌面淨空與螢幕淨空安全控管

5.13.1 個人電腦、伺服器或主機應設定螢幕密碼保護程式，螢幕保護程式啟動時間設定不應超過 10 分鐘。

5.13.2 下班時應關閉不需使用之個人電腦。

5.13.3 應實施桌面淨空，重要文件應妥善保管。

6 參考文件

6.1 資訊資產管理規定。

6.2 資訊安全存取管理規定。

6.3 資訊安全事件通報管理規定。

6.4 資訊安全營運持續管理規定。

6.5 電腦機房門禁卡使用登記表。

6.6 電腦機房廠商進出管制登記表。

6.7 異常事件紀錄表。

6.8 設備進出紀錄表。
6.9 資訊作業委外安全管理規定。
6.10 委外廠商保密切結書。