德明財經科技大學

資訊作業管理規定

機密等級：一般

文件編號：Takming-ISMS-B-012

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	8	執行小組	增加”廠商”二字
1.2	113.02.29	6	執行小組	1.增加項目 5.7.1.6 2.項目 5.7.2.1 改為 6 個月
1.3	115.05.26	8,9	推動小組	新增 5.11 組態管理

1. 目的

為確保德明財經科技大學(以下簡稱本校)有效管理資訊系統與設備維運安全與運作效率，以符合資訊安全相關規範要求。

2. 適用範圍

本校辦公室與電腦機房之內與外部資訊設備，以及委外開發、自行開發與套裝軟體均適用。

3. 名詞定義

3.1. 資訊設備

泛指電腦設備(如筆記型電腦、個人電腦、伺服主機)、資訊週邊設備(如印表機、磁帶機等)、網路通訊設備(如路由器、交換器等)與傳真機、影印機等。

3.2. 服務水準協定(Service-Level Agreement, SLA)

指服務提供者與使用者之間所訂定的協定，双方可以透過 SLA 的協調進行，以取得對於使用者需求、服務內容及保證的共識。

3.3. 可攜式設備

可攜帶且具備運算處理或資料擷取功能之電子設備，例如：筆記型電腦、照相機、照相手機、攝影機、燒錄器、磁帶機等。

3.4. 可攜式媒體

可攜帶之儲存媒體，例如：磁片、磁帶、記憶卡、光碟片、隨身碟、外接式硬碟等。

3.5. 軟體

指本校資訊資產分類中「電腦軟體」之電腦程式及電腦程式之存放媒體(如磁碟片、光碟片等)。

4. 權責

4.1. 主機管理人員

4.1.1. 確保主機系統之安全管理，以維護主機系統之機密性、完整性與可用性。

4.1.2. 如遇資訊安全事件，須依照「資訊安全事件通報管理規定」進行通報。

4.1.3. 應分析系統與應用程式之網路存取行為以提供網路設備、防火牆安全規則設定之參考資訊。

4.2. 防毒系統管理人員

4.2.1. 定期確認病毒碼為最新版本。

4.2.2. 追蹤主機及個人電腦是否安裝最新病毒碼。

4.2.3. 處理電腦病毒問題。

4.3. 本校軟體管理人員

4.3.1. 協助軟體採購申請作業。

4.3.2. 負責保管大量軟體授權證明與安裝光碟。

4.3.3. 管制本校大量授權軟體使用情形。

5. 要求事項

5.1. 文件化作業程序的管理要求

組織為落實資訊資產的存取授權能有效控管，將營運流程中相關的控管要求訂定相關辦法或管理要點。

5.2. 變更管理

5.2.1. 評估系統變更之程序

5.2.1.1. 評估系統變更對各應用系統或服務導致之影響。

5.2.1.2. 評估可使用之資源，包括供測試用之硬體設備、人員調度、廠商支援等。

5.2.1.3. 變更執行前，與各設備、系統人員進行充分協調及溝通，以利變更計畫之執行。

5.2.2. 擬定變更計畫

若屬系統設定及維護之變更則填寫「電算中心軟硬體需求服務申請表」，若變更會造成系統或服務之影響，則須詳列變更項目清單(格式不拘)，評估、安排變更所需之人員及時程(加變更計劃表(格式不拘))。

5.2.3. 變更計畫核准

所有系統變更須經過權責主管核准。

5.2.4. 變更前環境及設定之備份

變更計畫執行前須將原先舊環境之程式、資料及設定檔予以完整備份。

5.2.5. 變更計畫執行及監督

指派該主機管理人員執行，並依照擬定計畫進行監督。

5.3. 容量管理

5.3.1. 機房與主機管理人員應對資訊系統、資訊設備之資源使用狀況進行檢查記錄於「巡查紀錄表」中。

5.3.2. 依據資通訊設備資源使用狀況及資源容量之需求，適時進行系統調整與系統容量擴充規劃，以確保獲得必要之系統作業資源。

5.3.3. 系統容量評估與規劃時，須注意硬體設備及軟體系統版本更新、使用與維護之生命週期，及硬軟體系統運作相容性。

5.4. 應用系統測試/正式環境、資料庫之安全維護

5.4.1. 應將敏感性系統隔離，並明確識別應用系統的敏感性並加以文件化。

5.4.2. 在共用環境中執行敏感的應用程式時，宜識別各共用資源的應用系統與其對應的風險。

5.4.3. 測試環境所使用之設備環境應予獨立，不應與提供線上服務之設備環境共用。

5.5. 防範惡意軟體

5.5.1. 電腦病毒預防

5.5.1.1. 本校伺服器與個人電腦皆須安裝防毒軟體，並應啟動即時病毒防範機制，並至少每週完整掃描一次。

5.5.1.2. 提交個人電腦或筆記型電腦給使用者前，須安裝至最新之修補程式及病毒碼，並即時修補相關安全漏洞。。

5.5.1.3. 正確配置瀏覽器之安全設定，建議設定在中級風險等級(含)以上。

5.5.1.4. 電子郵件須先經過防毒軟體掃描，並禁止開啟來路不明之檔案或電子郵件及其附加檔案，以避免遭受病毒攻擊。

5.5.1.5. 本校以電子郵件病毒閘道器提供主動及全面性的防範，避免病毒及電腦蠕蟲以信件型態傳染。

5.5.1.6. 非本校擁有之電腦欲進行網路連線時，依據「資訊安全存取管理規定」辦理，經核准後，始可與內部網路連接。

5.5.1.7. 如需使用外來的可攜式設備或媒體，應確認設備未遭受病毒感染。

5.5.1.8. 重要資料應定期備份。

5.5.2. 電腦病毒處理

5.5.2.1. 如遇疑似中毒情況，防毒軟體無法解毒或作業仍不正常時，應依據「資訊安全事件通報管理規定」通報權責單位進行報修，並通知相關廠商協助處理。

5.5.2.2. 確認為中毒事件後，應判斷感染途徑及其病毒名稱，並應立刻協助使用者將病毒解除或隔離。

5.5.2.3. 當電腦病毒無法移除或隔離時，應將電腦關機，並中斷網路連線，如無法短時間內處理，則重建使用者作業環境並利用備份還原資料。

5.5.2.4. 如產生大規模電腦病毒感染，並有擴散情形，應需立即中斷相關設備之網路連線，防止病毒透過磁碟共享途徑傳染。同時應依據「資訊安全事件通報管理規定」通報權責單位，直到處理完成後始得復原。

5.5.2.5. 防毒系統管理人員遇電腦病毒無法移除或隔離時，應將電腦離線並通知防毒系統廠商處理。

5.5.2.6. 解毒完成後，需協助使用者了解受損情形提供改善方式給使用者，並將感染途徑、病毒名稱、處理結果及受損情況記錄。

5.6. 資訊備份

5.6.1. 備份管理原則

5.6.1.1. 若備份目標檔案資料量大且異動不頻繁或完整備份需大

量備份媒體時，應採取使用差異備份，並於適當週期執行完整備份。目前採取方式為每日進行差異備份，每周進行完整備份。

5.6.1.2. 如備份目標異動頻繁且備份作業會影響系統效能，則採取備份於本機儲存媒體，或將需備份之目標複製至備份集中儲存區，視情況再將備份檔案寫入備份媒體。

5.6.1.3. 備份行為需跨網路進行時，應避免使用流量高之網路區段，盡可能使用獨立之網路區段進行備份或是用其他通訊架構進行備份。

5.6.1.4. 規劃備份時應包含系統設定、應用程式、資料庫備份等項目。

5.6.1.5. 直接對使用中之系統或是檔案進行備份時，需先考量備份過程中可能影響之範圍與情況。

5.6.1.6. 備份後之備份媒體保管，依據「資訊資產管理規定」文件，按其機密等級進行控管。

5.6.2. 備份作業程序

5.6.2.1. 備份負責人依據備份計畫，進行備份作業。

5.6.2.2. 週期性備份作業、備份結果之相關作業紀錄須留存備查。

5.6.2.3. 非專案之備份需求，應另行規劃備份機制。

5.6.2.4. 備份作業之結果須於每日進行機房檢查時，於「備份檢查紀錄表」中記錄，並載明備份成功與否及原因。

5.6.3. 例行性備份作業

5.6.3.1. 資料庫備份

備份作業規劃若為日備份，則至少每週進行完整備份到備份媒體上，除有特殊要求外，此作業每次備份之完整備份至少保留三代。

5.6.3.2. 作業系統備份

5.6.3.2.1. 單機無備援或無設置 RAID 架構之主機，應採取磁碟鏡像(Mirror)或是磁碟影像檔方式進行作業系統備份。

5.6.3.2.2. 作業系統若有異動，須進行完整資料備份，此作業每次備份之資料保留二代。

5.6.3.3. 應用系統備份

5.6.3.3.1. 具有安裝程式之應用系統，須至少備份應用系統之設定檔案。

5.6.3.3.2. 如有異動須對應用系統進行完整資料備份，此作業每次備份之資料保留二代。

5.6.3.4. 通訊網路系統設定備份

5.6.3.4.1. 通訊網路系統相關設定檔需以適當方式進行備份。

5.6.3.4.2. 系統設定如有異動，須進行完整性備份，每次備份保留二代。

5.6.4. 臨時性備份

5.6.4.1. 當遇有硬體更換、軟體更新或升級或其他有資料安全顧慮上之特殊情形時，須進行臨時性資料備份，以確保作業過程中如發生意外狀況導致系統失效或資料遺失，仍能順利回復至變更前狀態。有關變更相關規範，依據「資訊應用系統安全管理規定」文件之變更管理相關章節辦理。

5.6.4.2. 臨時性備份作業完成後，應立即執行備份資料檢查作業，確保備份資料之可用性。

5.6.4.3. 在此備份作業應考量在不影響例行性備份作業下進行。

5.6.5. 備份資料檢查與復原

5.6.5.1. 備份負責人應定期排定檢查時機並記錄於「備份檢查紀錄表」，以確保備份媒體之可讀性。

5.6.5.2. 關鍵業務系統備份資料應至少每年執行資料回復測試，以確認備份資料之可用性。

5.6.5.3. 系統毀損依據「資訊安全營運持續管理規定」文件進行復原。

5.6.5.4. 復原作業應記錄回存所需時間，以供緊急應變計畫參考。

5.6.6. 備份作業異常處理

5.6.6.1. 如備份作業過程中發生異常狀況，備份負責人應向系統負責人與主管呈報。

5.6.6.2. 系統負責人應告知異常原因，處理方法及結果，並由備份負責人記錄並檢附於「備份檢查紀錄表」中。

5.6.7. 備份媒體與備份設備使用、維護及報廢。

5.6.7.1. 備份媒體保管人應檢查備份媒體使用狀況，並且汰換超過使用年限之備份媒體。

5.6.7.2. 備份媒體使用、報廢、銷毀時，應由備份媒體保管人依據「資訊資產管理規定」文件辦理，避免資訊外洩。

5.6.7.3. 運送備份媒體時，應將備份媒體放置於具防護功能的設備內予以保護。

5.7. 存錄及監視

5.7.1. 稽核存錄

5.7.1.1. 組織應依據應用系統的重要性，執行監控作業。

5.7.1.2. 應針對重要系統，在不影響效能運作下開啟相關日誌包

括：

5.7.1.2.1. 事件（成功或失敗）發生的時間，

5.7.1.2.2. 事件的資訊（如已處置檔案）或失效的資訊（如已發生錯誤並採取矯正措施）。

5.7.1.2.3. 所涉及的帳號和管理者或操作者。

5.7.1.3. 應用系統有提供記錄功能應予啟動，若無則視系統之重要性，以書面方式記錄之。除預設之系統記錄功能外，應考量記錄以下事件：

5.7.1.3.1. 系統管理者及具備特殊權限帳號之登入成功及失敗事件紀錄。

5.7.1.3.2. 使用者帳號異動及對密碼檔案之讀取與變更。

5.7.1.3.3. 變更正式應用系統的程式原始碼及程式執行碼。

5.7.1.3.4. 對於作業系統設定檔之存取及變更。

5.7.1.4. 各系統的系統紀錄存取，應限定僅由系統管理者或具讀取權限者存取。

5.7.1.5. 資訊設備保管單位應於每工作日檢核各設備之運作狀況，發現異常時，應填寫「異常事件紀錄表」並進行必要之處置。

5.7.1.6. 各類型系統紀錄應予妥善保存，保存期限至少 6 個月。

5.7.2. 日誌資訊保護的控制措施

5.7.2.1. 系統需開啟系統日誌及適當稽核記錄功能，並將關鍵性系統主機之紀錄匯出存檔備查，並保留至少 6 個月。

5.7.2.2. 主機管理人員需確實檢視系統日誌(含各式通訊服務之連線紀錄)、系統資源使用狀態、系統漏洞與修補程式安裝情形。

5.7.3. 管理者與操作者日誌

5.7.3.1. 資通訊設備、應用系統與資料庫之管理者與操作者所有執行的管理或異動作業，應加以記錄。

5.7.3.2. 系統管理者與操作者日誌應定期予以審查。

5.7.4. 資訊與通信設備時間同步

5.7.4.1. 資訊設備及主機伺服器應盡可能與單一參考時間源同步。以確保系統時間的一致性。

5.7.4.2. 資訊設備如無法設定單一參考時間源，則應約定同步之時間源，由設備管理員定期(至少每季一次)或於設備異動時進行系統時間同步作業。

5.8. 運作中系統之軟體安裝

5.8.1. 個人使用之電腦嚴禁安裝未經授權之軟體，若需安裝新軟體，

取得授權後，方可進行相關作業與設定。

5.8.2. 執行套裝軟體之昇級或汰換作業時，應注意新舊版之相容性、資料之備份及確保原作業環境之正常運作等事宜。

5.8.3. 資訊設備系統更新與漏洞修補

5.8.3.1. 資訊設備系統應定期進行系統弱點掃描並針對各設備發現之弱點執行必要性、可行性分析及修補之風險評估作業，以做為是否修補之依據。

5.8.3.2. 主機系統、網路設備、軟硬體廠商發佈之系統相關之修正程式(Patch)，系統負責人應督導設備維護廠商執行修正程式之必要性、可行性分析及風險評估作業，進行修補。

5.8.3.3. 伺服器由系統管理人員評估必要性、可行性分析及風險評估作業後，安裝必要之補強項目，以避免系統安全漏洞發生。

5.9. 技術脆弱性管理

5.9.1. 系統安全性更新及修正

5.9.1.1. 留意國內外危機處理中心(TWCERT)宣佈重大安全弱點及廠商發佈之修正檔訊息。通知廠商或自行取得修正程式。

5.9.1.2. 主機系統、網路設備、軟硬體廠商發佈之系統相關之修正程式(Patch)，系統負責人應督導設備維護廠商執行修正程式之必要性、可行性分析及風險評估作業，進行修補。

5.9.1.3. 與系統安全相關之修正程式應適時進行修補，必要時由廠商於測試後協助安裝；其他額外功能則視實際需求選擇性安裝。

5.9.1.4. 系統上線前應完成必要之漏洞修補作業，相關作業完成後，需重新關閉因修補作業而開放之非必要網路服務。

5.9.1.5. 關鍵性主機於安裝修正程式前，需先行測試並詳細記錄修正程序，確認系統穩定運作無誤後，方可於正式主機進行修正。

5.9.2. 系統平台作業要求

5.9.2.1. Windows 平台作業要求

(1) 取消、停用「Guest」帳戶或變更「Guest」帳戶之名稱。

(2) 建立 NTFS 檔案系統達成檔案系統權限管制。

(3) 主網域控制站上啟用稽核原則，如：登入失敗之稽核，以保留系統稽核軌跡。

5.9.2.2. UNIX/Linux 平台作業要求

(1) 關閉匿名權限帳戶可存取範圍。
(2) 在主機上啟用稽核原則，如：登入失敗之稽核，以保留系統稽核軌跡。

5.10. 軟體安裝之限制

5.10.1. 軟體管理

5.10.1.1. 本校員工因業務須增置軟體者，須填寫請購單或以簽呈方式經單位主管核可後，移送採購組辦理採購。

5.10.1.2. 為有效控制「免費軟體」或「共享軟體」的使用，使用人員須事先瞭解其相關版權規定。

5.10.1.3. 以專案委外方式開發併同引進之軟體不列入此規範，由各別專案納入列管。

5.10.1.4. 軟體採購後，由本校軟體管理人員或工程師協助安裝，或由軟體使用者自行安裝。

5.10.1.5. 本校員工不得任意自行安裝及散佈未經授權之軟體。

5.10.1.6. 個人申請軟體之相關授權文件、軟體使用手冊與軟體原始存放媒體，應由使用人保管。

5.10.1.7. 大量申請軟體之相關授權文件、軟體使用手冊與軟體原始存放媒體，應由軟體管理人員集中保管。

5.10.1.8. 軟體管理人員應定期執行軟體清查，並更新「軟體使用管理表」。

5.11. 組態管理

5.11.1. 自訂組態基準

5.11.1.1. 應最大限度符合本校系統獲取開發與維護作業規範，並留下開發與版次變更紀錄。

5.11.1.2. 自行或委外建置組態基準，應可書面記錄、實作、監視並審查硬體、軟體、服務（含雲端服務）、網路、新安裝之系統以及運作中之系統，並符合安全系統發展生命週期(SSDLC)之要求。

5.11.2. 標準組態基準

5.11.2.1. 建立標準組態基準時，應依照下列原則與注意事項進行之

5.11.2.1.1. 使用依據開發商所提供之操作指引或公開說明書。

5.11.2.1.2. 宜考量本校之資通安全等級與保有之資料進行設定。

5.11.2.1.3. 宜考量本校之資訊安全政策、法令法規要點指引及其他安全要求事項。

5.11.2.1.4. 宜考量在組織全景中，標準組態基準之可用性與適用性。

5.11.2.2. 應考量新型威脅弱點、系統更新或硬體更新，必要時更新標準組態設定。

5.11.2.3. 應定期審查標準組態設定之妥適性。

5.11.2.4. 於設定標準組態基準時，應依照下列原則與注意事項進行之

5.11.2.4.1. 將具有特權或系統管理員等級之存取權限的身份數量減至最少。

5.11.2.4.2. 停用不必要、未使用或不安全的身份。

5.11.2.4.3. 停用或限制非必要的功能和服務。

5.11.2.4.4. 限制對強效公用程式和主機參數設定之存取權限。

5.11.2.4.5. 鐘訊同步。

5.11.2.4.6. 安裝後，立即變更廠商預設鑑別資訊，如預設密碼，並審查其他重要的預設安全相關參數。

5.11.2.4.7. 應設定無動作逾時自動登出機制。

5.11.2.4.8. 查證是否為授權使用。

5.11.3. 安全組態管理

5.11.3.1. 所建立之安全組態，應可書面記錄、實作、監視並審查，應維護組態變更日誌，並對安全組態設定進行備份。

5.11.3.2. 組態紀錄宜包含下列內容

5.11.3.2.1. 資產擁有者或聯絡窗口資訊

5.11.3.2.2. 前次組態變更日期

5.11.3.2.3. 標準組態之版本

5.11.3.2.4. 與其他安全組態之關係

5.11.3.2.5. 未規範之組態基準要求，則依照我國資通安全相關法令、規定、或要點指引實施之。

6. 參考文件

6.1. 政府採購法。

6.2. 資訊資產管理規定。

6.3. 資訊應用系統安全管理規定。

6.4. 資訊作業委外安全管理規定。

6.5. 資訊安全存取管理規定。

6.6. 資訊安全事件通報管理規定。

6.7. 資訊安全營運持續管理規定。

6.8. 電腦機房廠商進出管制登記表。
6.9. 電算中心軟硬體需求服務申請表。
6.10. 委外廠商保密切結書。
6.11. 軟體使用管理表。
6.12. 備份檢查紀錄表。
6.13. 巡查紀錄表。
6.14. 異常事件紀錄表。