德明財經科技大學

通信與作業管理說明書

機密等級：一般

文件編號：Takming-ISMS-C-002

版　　次：V1.1

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	114.02.08		推動小組	“電子計算機人員”改為”本校所有使用資訊系統與網路環境之人員皆”，”敏感”改為”限制使用”

1. 目的

德明財經科技大學（以下簡稱本校）為確保資訊系統與網路環境之安全性、可用性及完整性，特訂定「通信與作業管理說明書」（以下簡稱本說明書）以資遵循。

2. 適用範圍

本校實施資訊安全管理系統(ISMS) 內相關網路服務及設備之管理。

3. 名詞定義

無。

4. 權責

本校所有使用資訊系統與網路環境之人員皆應遵守本說明書之相關規定，以確保資訊系統及網路之安全。

5. 要求事項

5.1 作業說明

5.1.1 應建立資訊系統之安全控管機制，以確保資訊資料之安全，保護系統及網路作業，防止未經授權之系統存取。

5.1.2 資訊系統與網路管理責任應加以區隔，足以影響業務經營管理的資訊，不可只由單獨一人知悉。如因人力資源限制，無法區隔責任，則應加強監督與稽核等措施。

5.1.3 應用程式之執行、資料庫之維護及相關作業系統與網路硬體資源應分派管理人員。

5.1.4 網路管理人員應妥為規劃網路架構、設定網路參數，並依規定備份相關檔案。

5.1.5 應規劃系統與設備的開發與測試環境，避免於已上線運作設備及環境進行開發或測試工作。

5.1.6 系統及設備建置前，單位應對系統需求做適當規劃，以確保足夠的電腦處理及儲存容量。如需委外開發或採購，則依「資訊系統開發及維護說明書」辦理。

5.1.7 系統設備與軟體之建置，均應依照「資訊系統開發及維護說明書」進行測試及驗收。

5.2 變更管理

5.2.1 新增設備及網路變動，應即時修改網路架構圖及設備資料。

5.2.2 網路架構變動之影響性甚大者應經權責單位主管以上核准。

5.2.3 新增對外網路連線，需注意安全性考量，從嚴審核對外網路連線與內部之連接方式。

5.2.4 如有廠商參與安裝或設定，應陪同參與並記錄。

5.2.5 相關手冊變更時（如操作文件、參考文件或作業準則），應同步修改維護相關文件。

5.3 電腦軟體與程式著作權保護

5.3.1 應訂定使用授權軟體與遵守著作權規範，違反規範者應依相關程序懲處。

5.3.2 使用軟體與資訊產品不得超過允許的最高使用人數。

5.3.3 使用軟體與資訊產品應遵守相關規定，例如限制於指定之機器使用、限制僅於備份時方可複製等。

5.3.4 取得之合法軟體不得從事或轉讓予非授權範圍之使用。

5.3.5 從公共網路取得之合法軟體與資訊須遵守原著作權者、個人資料保護法 之規定。

5.3.6 應妥善保管採購軟體產品之授權書、原版光碟、手冊等等證明。

5.3.7 經由網際網路下載之公開授權軟體，應在確認安全無虞及不違反智慧財產權前提下，方得下載執行。

5.4 網路安全管理

5.4.1 避免利用公共網路傳送限制使用等級以上資訊，應保護資料在公共網路傳輸之完整性及機密性，並保護連線作業系統之安全性。

5.4.2 網路管理人員應利用網路管理工具，偵測及分析網路流量。

5.4.3 因業務需要開放相關人員從遠端登入內部網路系統之網路服務，應執行嚴謹之身分辨識作業，或提供連線設備之識別機制。

5.4.4 網路管理人員除依相關法令或規定，不得閱覽使用者之私人檔案；但如發現有可疑之網路安全情事，網路系統管理人員得依授權規定，使用工具檢查檔案。

5.5 網路使用者之管理

5.5.1 經授權之網路使用者，只能在授權範圍內存取網路資源。

5.5.2 網路使用者於使用行動碼（如 active X, java applet）之前，應先確認其授權資料，並禁止執行未經授權之行動碼。

5.5.3 網路使用者應遵守網路安全規定，並確實瞭解其應負之責任；如有違反網路安全情事，應依資訊安全規定，限制或撤銷其網路資源存取權利，並依相關規定處理。

5.5.4 網路使用者不得將自己之登入身分識別與登入網路之密碼交付他人使用。

5.5.5 禁止網路使用者以任何方法竊取他人之登入身分與登入網路通行碼。

5.5.6 禁止網路使用者以任何儀器設備或軟體工具竊聽網路上之通訊。

5.5.7 禁止網路使用者在網路上取用未經授權之檔案。

5.5.8 網路使用者不得任意修改網路相關參數。

5.5.9 為維護本中心網路安全，網路管理人員於發現網路使用者之電腦發送異常封包或使用非經允許之服務時，得中斷其網路使用權

限，至改善為止。

5.6 防火牆之安全管理

5.6.1 所有與外界網路連接之連線，均應透過加裝防火牆，以控管外界與本中心內部網路間之資料傳輸與資源存取。

5.6.2 防火牆應由管理人員執行控管設定，建立包含身分辨識機制與系統稽核之安全機制。

5.6.3 防火牆設置完成時，應測試防火牆是否依設定之功能正常及安全地運作。如有缺失，應立即調整系統設定，直到符合既定之安全目標。

5.6.4 管理人員應配合資訊安全政策及規定之修正，以及網路設備之變動，隨時檢討及調整防火牆系統設定，調整系統存取權限，以反映最新狀況。

5.6.5 應視業務需要及設備功能，對於通過防火牆之特定網路服務，應予確實紀錄。

5.6.6 管理人員應避免採取遠端登入方式登入防火牆主機，以避免登入資料遭竊取，危害網路安全。如果必須使用遠端登入方式管理，應訂定嚴謹之遠端登入控管措施。

5.6.7 若資源許可應建立防火牆設備之備援機制；防火牆之環境建置檔等需定期執行備份作業。

5.6.8 防火牆政策、設定、物件及規則應每年定期覆核，並記錄於「防火牆規則查檢表」中。

5.6.9 管理人員每月將防火牆之組態設定(config)轉出存放於備份機器上，並記錄於「備份檢查記錄表」。

5.6.10 每年檢視各防火牆內之黑白名單，若已屆期限或該 IP 不再使用，請系統負責人確認後刪除。

5.7 網路資訊之管理

5.7.1 限制使用等級及機密等級之業務資料或文件不得存放於對外開放之資訊系統中，若因特殊業務功能之需求，必須採取加強之安全管控機制，如：資料加密。

5.7.2 網路管理人員應負責監督網路流量及使用情形，並對可能導致系統作業癱瘓等情事，預作有效的防範，以免影響網路服務品質。

5.7.3 對外開放的資訊系統所提供之網路服務，如：HTTP、FTP 等，應採取適當之存取控管機制。

5.7.4 對外開放的資訊系統，如：存放教職員、學生或家長申請或註冊之個人資料檔案，其傳輸過程應以加密方式處理，並妥善保管資料，以防止被竊取或移作他途之用，侵犯個人隱私。

5.7.5 網路管理人員於偵測收到資訊系統異常狀況或駭客入侵之警示訊

息時，應立即通報權責主管，依據相關作業管理規範採取適當之緊急應變處理，並留存系統異常處理紀錄。

6.參考文件

6.1 資訊安全政策。

6.2 防火牆規則查檢表。

6.3 備份檢查記錄表。