德明財經科技大學

網路安全管理規定

機密等級：一般

文件編號：Takming-ISMS-B-008

版　次：V 1.2

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	6	推動小組	增加”、「新進人員資安宣導單」、「員工個資保密同意書」”
1.2	115.06.10	6	推動小組	增加資料洩漏預防(DLP)

1. 目的

為確保德明財經科技大學(以下簡稱本校)網路資料傳輸及相關設備之安全保護，透過程序化之安全控管機制，防止未經授權及不當的網路使用行為。

2. 適用範圍

本校負責之網路設備及相關人員。

3. 名詞定義

無。

4. 權責

4.1. 網路管理人員

4.1.1.確保網路資源之安全管理，以維護其機密性、完整性與可用性。

4.2. 權責主管

4.2.1.負責核准相關設備使用、連線之申請，並督導網路設備之安全管理。

5. 要求事項

5.1. 網路安全管理

5.1.1.網路使用者安全管理

5.1.1.1.需經授權並賦予相關存取權限後，始得使用網路資源。

5.1.1.2.禁止以任何儀器設備或軟體工具竊聽網路上的通訊。

5.1.1.3.不得以任何手段蓄意干擾或妨害網路系統的正常運作。

5.1.1.4.禁止濫用網路系統，若影響網路正常運作者，得暫停其使用權利。

5.1.1.5.使用者若發現疑似網路安全事件，依據「資訊安全事件通報管理規定」進行通報。

5.1.2.網路頻寬管理

5.1.2.1.應進行網路流量之監控，保障網路頻寬之正常使用。

5.1.2.2.網路管理人員如發現流量異常，應立即採取適當措施後，分析網路異常原因。如果為使用者非法使用或是電腦中毒，依據「資訊安全事件通報管理規定」進行通報，並通知相關人員進行後續處理。

5.1.3.防火牆安全管理

5.1.3.1.防火牆管理原則

5.1.3.1.1. 防火牆應開啟記錄功能，記錄連線狀況。

5.1.3.2.防火牆過濾規則設定管理

5.1.3.2.1. 除由指定 IP 位址及特定的連接埠登入管理外，其它人員均不得管理防火牆。

5.1.3.2.2. 來源 IP 位址、目標 IP 位址與網路服務之群組設定，應與申請需求相符合。

5.1.3.2.3. 優先考慮使用正面表列，並應於過濾規則最後設置

拒絕全部服務的規則。

5.1.3.2.4. 為避免邏輯上重複與繁瑣之過濾原則，導致防火牆效能低落，防火牆規則應每年進行檢視，以確保其適切性。

5.1.3.2.5. 網路使用者需配合提供存取控制設定之參考資訊。

5.1.3.3.防火牆規則異動管理

5.1.3.3.1. 防火牆規則異動應由申請人填寫「網路服務連線申請表」提出防火牆規則異動需求申請，經權責主管或其代理人簽名或蓋章後交相關業務承辦人辦理。

5.1.3.3.2. 網路管理人員異動規則時，應依據「網路服務連線申請表」作業，並考量是否可以與其他規則整併，處理結果中並註明對應之防火牆規則 ID。

5.1.3.3.3. 異動規則前應進行測試或是紙上推演，以確認異動之規則可正確工作。

5.1.3.4.防火牆備份與韌體更新管理

5.1.3.4.1. 備份防火牆上設定及規則，請參考「資訊作業管理規定」，並應有適當的回復程序。

5.1.3.4.2. 當有新的韌體更新程式發佈時，在不影響正常營運的前提下，經測試無誤後，應更新防火牆韌體程式。

5.1.3.4.3. 重要之防火牆應有備援設備。

5.1.3.5.防火牆紀錄管理

5.1.3.5.1. 針對防火牆紀錄中之異常狀況，應依據「資訊安全事件通報管理規定」進行通報及處理。

5.1.3.5.2. 防火牆紀錄應定期匯出存放，以利日後追蹤使用。

5.1.3.5.3. 除網路管理人員，防火牆紀錄之調閱應經授權。

5.2. 網路設備安全管理

5.2.1.網路控制措施

5.2.1.1.網路管理人員應於網路設備及主機系統中限制不當的網路服務功能與通訊協定如：NetBIOS、Microsoft-DS 等，而開放其他正常的網路服務功能與通訊協定，如：HTTP、FTP 等。

5.2.1.2.路由設備之存取控制清單，若變更限制條件時，應保留相關備份設定檔，以利日後異常追蹤。

5.2.1.3.路由設備管理員應定期檢視設備是否存在漏洞，若有漏洞，應立即通知廠商或取得合法修正程式後，進行修補。

5.2.2.網路連接設備安全

5.2.2.1.密碼設定

5.2.2.1.1. 於設定密碼前，應啟動密碼加密功能，網路連接設

備不得使用明碼儲存密碼。密碼管理方式依據「資訊安全存取管理規定」辦理。

5.2.2.2.維護存取控制清單

5.2.2.2.1. 依照每個網路介面用途及通訊協定，設定存取控制清單，以便進行存取控制。

5.2.2.2.2. 需使用遠端方式管理網路連接設備時，應於網路連接設備中設定適當之存取控制清單，限制遠端管理之來源 IP 位置。

5.2.2.2.3. 網路設備之存取控制清單應適當保存（格式不拘）並至少保留 3 個月存查，以利日後異常之追蹤。

5.2.2.3.網路服務申請，應每六個月定期覆核。

5.2.3.網路通訊設備管理

5.2.3.1.網路通訊設備之安裝、測試或維護改善，其工作內容應有詳細紀錄。

5.2.3.2.網路通訊設備安裝、維護前須與廠商或相關人員進行協調，以充分了解該項作業之影響層面，實際進行作業時並請廠商提供到場協助。

5.2.3.3.網路通訊設備安裝應考慮裝置場地之安全性，儘可能設置於有門禁管制之地點，並考慮通風散熱問題。

5.2.3.4.為維持網路的持續正常運作，重要網路通訊設備應有備援設計或備品並應加裝不斷電系統(UPS)。

5.2.3.5.網路通訊設備應定期維護檢查軟硬體相關工作。

5.2.4.網路佈線安全管理

5.2.4.1.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。

5.2.4.2.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。

5.2.4.3.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。

5.2.5.啟用網路設備記錄服務

5.2.5.1.重要網路設備應啟動記錄功能，並將紀錄蒐集保存以便追蹤判讀。

5.3. 網路服務安全

5.3.1.網路服務安全管理

5.3.1.1.本校只開放必須的網路服務功能與通訊協定。如需異動，須經申請程序由相關人員進行安全評估，確定無安全之顧慮，經由權責主管核可後方得開放。

5.3.1.2.為確保網際網路的服務持續暢通，本校網路與外界網路的連接，應有備援線路，並確保備援線路受到安全管控。

5.3.1.3.本校之校園網路規範則依據「德明財經科技大學校園網路使用規定」辦理。

5.3.2.網路防毒與入侵偵測/防禦安全管理

5.3.2.1.網路防毒安全管理，依據「資訊作業管理規定」辦理。

5.3.2.2.應於網路重要區段或是節點，佈署網路入侵偵測/防禦系統，進行入侵偵測與防禦。

5.3.2.3.網路管理人員應配合資訊安全政策及規定，隨時檢討及調整網路入侵偵測/防禦系統的設定，以反應最新的狀況。

5.3.2.4.如發現疑似網路入侵情形，依據「資訊安全事件通報管理規定」辦理。

5.3.3.紀錄與蒐證安全管理

5.3.3.1.針對疑似網路入侵行為，應利用網路設備相關紀錄檔執行追蹤並進行防堵措施。

5.3.3.2.不得任意窺視使用者個人資料或進行其他侵犯隱私權之行為。

5.3.3.3.遵循相關法令要求。

5.3.3.4.違反本校資安規定者，依據「資訊安全事件通報管理規定」辦理。

5.3.4.遠端使用者的鑑別

5.3.4.1.使用遠端網路服務需先取得授權，填寫「網路服務連線申請表」註明開通之網路功能，並經單位主管或其代理人簽名或蓋章後交業務負責人辦理。

5.3.5.遠端診斷與組態埠的保護－關閉不必要的服務

5.3.5.1.為預防不明人士透過網路偵測工具來找出路由器中有運作的服務，進而對其漏洞展開攻擊，造成路由器無法正常運作，關閉網路設備不必要之服務與通訊協定，用以避免網路駭客刺探攻擊。

5.4. 網路區隔安全控管

5.4.1.為便於管理，防止不當網路存取行為與流量散佈，應規劃適當網路區隔，並且有效執行。

5.4.2.應區分主機與使用者工作內容，賦予適當網路區段之 IP 位址，以協助網路存取控制管理。

5.4.3.應將對外網際網路連線服務予以適當存取控制，防止機敏資料外洩。

5.5. 弱點掃描安全管理

5.5.1.弱點掃描作業

5.5.1.1.由資訊安全執行分組擬定弱點掃描計畫，並經資訊安全執行小組召集人同意後進行。

5.5.1.2.弱點掃描應使用合法工具，執行前應確認工具為最新版本，

並應做好存取控管措施。

5.5.1.3.執行掃描作業前，應通知相關負責人，以預為應變。

5.5.1.4.掃描作業至少每年執行一次。

5.5.2.弱點掃描報告與修補作業

5.5.2.1.弱點掃描後應產生弱點掃描報告。

5.5.2.2.弱點掃描報告格式不拘，但應包含下列內容：

5.5.2.2.1. 弱點掃描檢測時間。

5.5.2.2.2. 弱點掃描檢測範圍。

5.5.2.2.3. 弱點風險程度說明。

5.5.2.2.4. 安全弱點列表與建議修補措施。

5.5.2.3.掃描出之弱點應限期改善，並填寫「弱點處理報告單」，且於修補後進行複掃。

5.5.2.4.於安裝修正程式前，需先行測試並確認運作正常後，方可進行安裝。

5.5.3.殘餘弱點管理

5.5.3.1.弱點若因故無法修補，相關管理人員於「弱點處理報告單」說明無法修補之原因與防禦因應方法。

5.5.3.2.「弱點處理報告單」必須予以留存備查。

5.6. 資訊傳送政策與程序

5.6.1.視業務需要如須對外提供資料時，不論以任何型式，均應審視是否符合「個人資料保護法」或其他相關法令之規定。

5.6.2.資料需求申請人需配合本校、主管機關或相關法令需求辦理。單位有資料傳送之需求時，應填寫「電算中心軟硬體需求服務申請表」，經申請單位與處理單位之權責主管核准後，始能提供。

5.6.3.傳送級別為「內部使用」以上之資料，應依「資訊資產管理規定」辦理，並僅得使用於申請目的之範圍，禁止移作他用。

5.6.4.傳送級別為「內部使用」以上之資料，其儲存媒體之管控應依據「資訊資產管理規定」辦理。

5.6.5.傳送級別為「內部使用」以上之資料，若須使用傳真方式回覆，應依據「實體環境安全管理規定」辦理。

5.7. 資訊傳送協議

5.7.1.合作廠商或各專案相關外部人員如有資訊設備連線、存取之需求，須填寫「網路服務連線申請表」，經單位權責主管核准後，由相關網路管理人員執行權限開放，適時監控。

5.7.2.合作廠商或各專案相關外部人員以遠端方式進行系統維護時，系統負責人必須隨時掌握系統維護狀況，如有任何異常狀況需立即通報權責主管知悉。

5.7.3.外部人員欲使用本校內部網路資源時，需由業務相關人員向網路管理人員提出申請，於審核後在規定時間至特定地點使用。

5.7.4.本校僅提供必要之網路服務項目、通訊協定，所有行為不得與本校原有之網路安全相關限制、規定相抵觸；若有特殊需求，則須經專案審查、評估核准後，方可建立連線與開放存取權。

5.8. 電子傳訊

5.8.1.電子郵件管控

5.8.1.1.使用本校電子郵件服務之人員均負有遵守此程序之責任，並應適當使用電子郵件，依據「德明財經科技大學校園網域帳號作業規定」辦理。

5.8.1.2.如對郵件傳遞內容的合法性有任何疑慮時，可洽詢相關權責主管或電子郵件系統管理人員。

5.8.1.3.若第三方欲檢視郵件紀錄，須行文校方核可後會本校電子計算機中心協同辦理。

5.8.1.4.限制使用(含)以上或密級之本校公文及資料，如需以電子郵件附件方式對外傳送，應編碼加密(如：RAR、ZIP 等)處理後傳送。

5.8.1.5.無論是內部互傳或對外的郵件皆不允許超過本校規定之大小限制，並禁止傳送垃圾郵件，以免影響頻寬，浪費網路資源。

5.8.1.6.本校視需要可對廣告信件進行攔阻。

5.8.1.7.依本校規定，進行電子郵件信箱容量及對外傳輸檔案大小之限制，電子郵件信箱容量如有特殊需求應填寫「電算中心軟硬體需求服務申請表」，經權責主管許可後，再由系統管理人員處理。

5.8.2.網路通訊服務傳遞

5.8.2.1.利用網路通訊服務，如電子郵件、即時通訊軟體或外部應用系統或資訊交換平台(如 FTP)時，應依據「資訊資產管理規定」，對不同等級的資訊資產傳遞要求，進行傳遞。

5.8.2.2.禁止使用網路通訊服務傳遞任何違法及違反本校規定之資訊。

5.8.2.3.透過本校應用資訊系統或平台進行資料相互流通時應保護，避免非授權人員取得機密性資料，應依據「資訊資產管理規定」與「資訊安全存取管理規定」，建立存取權限管理原則，並據以執行。

5.9. 網頁過濾

5.9.1. 網站類型識別與分級

5.9.1.1.根據營運需求和安全風險，將網站類型分級，例：

5.9.1.1.1. 允許存取：工作相關網站（內部服務、業務合作夥伴網站）。

5.9.1.1.2. 受限制：社交媒體、流媒體、娛樂及非工作相關的

網站。

5.9.1.1.3. 明確禁止：已知惡意網站、C&C 伺服器、散布非法或不當內容的網站。

5.9.1.2.定期參考威脅情資（如 URLhaus、Spamhaus），動態更新惡意網站清單。

5.9.2. 存取規則建立

5.9.2.1.設定存取規則：

5.9.2.1.1. 白名單：允許存取的特定域名或 IP 地址。

5.9.2.1.2. 黑名單：阻止存取的域名或 URL 關鍵字。

5.9.2.1.3. 基於類別的過濾：如根據內容類型（影音串流、下載）設限。

5.9.2.2.設置例外情況處理機制：對於業務需求，允許臨時或特殊的網站存取權限，需經主管核准。

5.9.3. 工具部署與配置

5.9.3.1.根據組織需求，選擇適合的(開源)工具進行部署，例如：

5.9.3.1.1. Squid Proxy + SquidGuard

5.9.3.1.1.1. 安裝 Squid 作為代理伺服器，集中控制所有網頁存取流量。

5.9.3.1.1.2. 配置 SquidGuard 過濾插件，導入白名單及黑名單規則，並設定類別過濾策略。

5.9.3.1.1.3. 啟用定期自動更新功能，保持規則與威脅情資同步。

5.9.3.1.2. Pi-hole

5.9.3.1.2.1. 部署 Pi-hole 作為內部網絡的 DNS 層過濾工具，攔截惡意網站的 DNS 查詢請求。

5.9.3.1.2.2. 配置主控節點 DNS 為 Pi-hole，並啟用自定義黑白名單功能。

5.9.3.1.2.3. 使用管理介面監控存取記錄，快速應對疑似惡意活動。

5.9.3.1.3. pfBlockerNG

5.9.3.1.3.1. 在使用 pfSense 的網絡中，啟用 pfBlockerNG 模組進行網絡層次的高級過濾。

5.9.3.1.3.2. 導入威脅清單（如 Emerging Threats），設定地理位置封鎖策略。

5.9.3.1.3.3. 啟用自動更新以確保過濾資料庫的時效性。

5.9.4. 網頁過濾運作與監控

5.9.4.1.監控與警報：

5.9.4.1.1. 配置工具生成日誌和警報（如發送阻止存取的即時通知）。

5.9.4.1.2. 定期檢視日誌，分析存取行為，及時調整策略。

5.9.4.2.教育與培訓：

5.9.4.2.1. 向教職員宣導網頁存取規範的重要性，以及惡意網站的威脅認知。

5.9.4.2.2. 結合實際案例，組織培訓活動，提升使用者安全意識。

5.9.5. 文件與記錄

5.9.5.1.網頁過濾策略文件。

5.9.5.2.過濾工具的配置檔案與更新記錄。

5.9.5.3.網頁存取日誌與封鎖記錄。

5.9.5.4.特殊存取許可的申請與審批文件。

5.9.6. 定期審查與改進

5.9.6.1.每半年或每當重大變更時，審核網頁過濾策略和工具的效果。

5.9.6.2.根據審核結果及安全事件，持續優化規則和工具配置。

5.10. 資料洩漏預防(DLP)

5.10.1. 靜態資料管理

5.10.1.1.掃描與標記敏感資料：使用 DLP 工具掃描儲存設備(伺服器、雲端等)，以定位敏感資料。

5.10.1.2.資料防護策略：加密或移動敏感資料到安全區域。

5.10.2. 傳輸中資料管理

5.10.2.1.實施網路流量監控：設置網路防護策略，阻止敏感資料通過非授權的管道(如郵件附件、FTP 上傳)。

5.10.2.2.郵件保護措施：為電子郵件啟用 DLP 篩查功能，阻止含有敏感內容的郵件外發。

5.10.3. 使用中資料管理

5.10.3.1.終端行為監控：阻止敏感資料複製至 USB 或截圖儲存。

5.10.4. DLP 策略建立與維護

5.10.4.1.建立基於角色的存取控制：僅授權用戶存取基於工作所需的最小資料集。

5.10.4.2.設置自動化處理規則：偵測到敏感資料外洩時，自動執行封鎖或加密。

5.10.5. 日誌與報告管理

5.10.5.1.紀錄資料洩漏事件：包括觸發規則、洩漏資料類型、發生位置等。

5.10.5.2.分系並改進策略：透過工具產出的報告，改進敏感資料防護機制。

5.10.6. 測試與演練

5.10.6.1.定期測試 DLP 策略，模擬資料洩漏事件，確保工具有效阻

止未經授權的資料外流。

5.10.7. 持續改進

5.10.7.1.根據監控結果與最新技術趨勢，定期更新 DLP 策略與工具版本。

5.11. 機密性協議

5.11.1.本校所聘(雇)用之內部及外部人員，應使其了解相關之工作責任與安全要求；本校同仁須簽署「員工工作同意書」、「新進人員資安宣導單」、「員工個資保密同意書」，外部人員簽署「委外廠商保密切結書」。

5.11.2.內部及外部人員離（調）職或合約終止時，應歸還於執行業務期間所擁有或使用之屬於組織的資訊資產。

6. 參考文件

6.1. 個人資料保護法。
6.2. 資訊資產管理規定。
6.3. 資訊安全存取管理規定。
6.4. 實體環境安全管理規定。
6.5. 資訊安全事件通報管理規定。
6.6. 資訊作業管理規定。
6.7. 網路服務連線申請表。
6.8. 弱點處理報告單。
6.9. 德明財經科技大學校園網路使用規定。
6.10. 電算中心軟硬體需求服務申請表。
6.11. 德明財經科技大學校園網域帳號作業規定。
6.12. 員工工作同意書。
6.13. 委外廠商保密切結書。
6.14. 防火牆規則查檢表。
6.15. 新進人員資安宣導單。
6.16. 員工個資保密同意書。