國立中央大學附屬中壢高級中學

通信與作業管理程序書

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要

目錄

1 目的

為防止國立中央大學附屬中壢高級中學（以下簡稱「本校」）資訊在不安全之網路環境下，遭致可能之破壞，或非預期及非經授權之修改，以確保資訊系統與資料之安全性、可用性及完整性。

2 適用範圍

本校所轄之範圍內，相關網路服務與設備及核心業務系統之管理。

3 權責

本校網路管理人員應遵守本程序書之相關規定，以確保本校網路之安全。

4 名詞定義

4.1 機密性 (Confidentiality)

確保只有經授權的人，才可以存取資訊。

4.2 完整性 (Integrity)

確保資訊與處理方法的正確性與完整性。

4.3 可用性 (Availability)

確保經授權的使用者在需要時可以取得資訊及相關資產。

4.4 可接受風險值

各類資訊資產之最低風險容忍度。

4.5 殘餘風險 (Residual Risk)

在採用相關控制措施之後剩餘的風險。

4.6 威脅 (Threat)

可能對系統或組織造成傷害之意外事件。

4.7 弱點 (Vulnerability)

因資訊資產本身狀況或所處環境之下，可能受到威脅利用而造成資產受到損害之因子。

4.8 風險 (Risk)

可能對團體或組織的資產發生損失或傷害的潛在威脅，通常利用弱點所產生之影響及發生可能性來衡量。

4.9 行動計算與通信設施

如筆記型電腦、掌上型電腦、行動電話等。

4.10 儲存媒體

如磁片、磁碟、磁帶、IC 卡、匣式磁帶、外接式硬碟、光碟、隨身碟、各式記憶卡、錄影帶、錄音帶等。

5 作業說明

5.1 資訊系統安全規劃作業

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 資訊系統管理職務與責任應加以區隔，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 伺服主機及網路設備應指定負責人，負責該主機之正常運作，包括應用程式之執行、資料庫之維護及相關作業系統與主機硬體資源之分配管理。主機或網路設備負責人無法進行管理時應由代理人負責，未指定負責人之主機及網路設備由機房管理負責人員負責。

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，主辦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「委外管理程序書」辦理。

5.1.7 系統設備與軟體之建置，均應依照「系統開發與維護程序書」之程序進行測試及驗收。

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 架構調整：架構變動之影響性甚大者應經資訊安全官以上核准，並遵循下列規定：

5.2.2.1 設備之功能性及設定方式應熟悉掌握。

5.2.2.2 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之方式。

5.2.2.3 如有廠商參與安裝或設定，必須全程陪同參與並記錄。

5.2.3 系統若有相關文件（如系統文件、參考文件或作業準則）時，系統相關負責人員於變更程序同時，應同步修改維護相關文件。

5.2.4 各項系統變更作業依據「系統開發與維護程序書」變更作業控制措施辦理。

5.3 惡意軟體之防範

5.3.1 禁止使用或下載未經授權或與業務無關之軟體。

5.3.2 應安裝病毒偵測與修復軟體，並定期更新病毒資訊，以防止病毒之攻擊。伺服器主機防毒軟體系統應設定主動掃瞄檢查，或由網路管理人員定期執行掃瞄檢查作業。

5.3.3 應定期檢查支援重要業務之作業系統是否有任何未核准的檔案或未經授權的修改。

5.3.4 應於使用來源不明、來源未經授權、或從未經信任網路接收之檔案前，檢查該檔案是否藏有病毒。

5.3.5 應於使用前檢查電子郵件附件和下載檔案有無惡意軟體。

5.3.6 使用者如偵測到電腦病毒入侵或其他惡意軟體，應立即通知系統或網路管理人員；管理者亦應將已遭病毒感染的資料及程式等資訊隨時提供使用者，以避免電腦病毒擴散。

5.3.7 系統或電腦設備如遭病毒入侵感染，應立即與網路離線並隔離，直到網路管理人員確認病毒已消除後，才可重新連線，並留存處理紀錄。

5.4 電腦軟體與程式著作權保護

5.4.1 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議處。

5.4.1.1 使用軟體與資訊產品不得超過允許的最高使用人數。

5.4.1.2 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。

5.4.1.3 取得之合法軟體不得從事或轉讓予非授權範圍之使用。

5.4.1.4 從公共網路取得之合法軟體與資訊須遵守原著作權者與電腦處理個人資料保護法之規定。

5.4.1.5 對公共系統的存取不得擅自存取其所相連的網路。

5.4.2 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。

5.4.3 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。

5.5 網路安全管理

5.5.1 網路服務之管理

5.5.1.1 避免利用公共網路傳送敏感等級（含）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。

5.5.1.2 網路管理人員應利用網路管理工具，偵測及分析網路流量。

5.5.1.3 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。

5.5.1.4 如果系統使用者為非合法授權之使用者時，應立即撤銷其系統使用權限；離（休、退）職人員應依資訊安全規定及程序，調整或終止其存取網路及系統之權限。

5.5.1.5 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。

5.5.1.6 網路管理人員除有緊急狀況外，未經使用者同意，不得增加、刪除及修改私人檔案。

5.5.1.7 網路設備軟硬體應限定由網路系統管理人員依規定辦理設定異動，並應留存紀錄備查。

5.5.1.8 對任何網路安全事件，網路管理人員應依「安全事件管理程序書」辦理。

5.5.1.9 網路管理人員應於每工作日檢查所有網路設備並記錄於「巡查紀錄表」，每月送主管簽核。如發現異常應依本程序之異常處理流程辦理。

5.5.2 網路使用者之管理

5.5.2.1 經授權之網路使用者，只能在授權範圍內存取網路資源。

5.5.2.2 網路使用者於使用行動碼（如 ActiveX、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。

5.5.2.3 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。

5.5.2.4 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。

5.5.2.5 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密碼。

5.5.2.6 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。

5.5.2.7 禁止網路使用者在網路上取用未經授權之檔案。

5.5.2.8 網路使用者不得將色情檔案建置在網路，亦不得在網路上散播色情文字、圖片、影像、聲音等不法或不當之資訊。

5.5.2.9 禁止網路使用者發送電子郵件騷擾他人，導致其他使用者之不安與不便；或以任何手段蓄意干擾或妨害網路系統之正常運作。

5.5.2.10 網路使用者不得任意修改網路相關參數。

5.5.2.11 為維護本校網路安全，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，依『校園網路使用規範』相關規定辦理。

5.5.3 無線網路使用之管理

5.5.3.1 無線網路基地台之使用應經適當控管。

5.5.3.2 無線網路設備之安裝設定應經核准。

5.5.3.3 無線網路設備之使用應取得授權，禁止於內部網路私自使用任何無線網路產品。

5.5.3.4 無線網路設備之使用應有適當管理機制，例如：授權使用之IP 數量、連接埠、網卡位址（MAC）過濾等。

5.5.3.5 無線網路之資料傳輸應使用加密機制，並就安全與資訊風險之考量，增加適當之防護機制以避免資料外洩。

5.5.4 防火牆之安全管理

5.5.4.1 所有與外界網路連接之連線，應透過加裝防火牆，以控管外

界與本校內部網路間之資料傳輸與資源存取。

5.5.4.2 防火牆設定異動時，應填寫「防火牆進出規則申請表」，經主管簽准後，交由網路管理人員設定。

5.5.4.3 防火牆應由網路管理人員執行控管設定，並依制定之資訊安全規定、資料安全等級及資源存取之控管策略，建立包含身分辨識機制與系統稽核之安全機制。

5.5.4.4 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。

5.5.4.5 網路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。

5.5.4.6 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。

5.5.4.7 網路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。

5.5.4.8 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。

5.5.4.9 防火牆政策及設定應每月定期覆核，並記錄於「巡查紀錄表」中，若已屆期限或該 IP 不再使用，請系統負責人確認後刪除，並填寫「防火牆進出規則申請表」。

5.5.4.10 網路管理人員每週將防火牆之 log 轉出存放於備份機器上，並記錄於「巡查紀錄表」。

5.5.4.11 於防火牆設定變更之前，將各防火牆之設定檔備份，並依「備份狀況紀錄表」之表列進行備份，存放於備份設備上。

5.5.5 網路資訊之管理

5.5.5.1 敏感等級（含）以上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。

5.5.5.2 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。

5.5.5.3 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。

5.5.5.4 對校外開放的資訊系統，如：存放教職員、學生或家長申請或註冊之個人資料檔案，其傳輸過程應考量以加密方式處理，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。

5.5.5.5 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。

5.5.6 網路管理作業流程

5.5.6.1 網路檢查作業

5.5.6.1.1 以指令方式 ping 各網段之 Gateway，以回應時間初步判斷網路狀態。

5.5.6.1.2 檢查防火牆之 log 及狀態。

5.5.6.1.3 防火牆發現異常情形應設定自動寄發通知信給網路管理人員，嚴重時網路管理人員應立即採取阻擋作為，並通知主管。

5.5.6.2 網路監控作業

5.5.6.2.1 利用工具自動 ping 各 IP，用以監控網路各節點，由其回

應數值判斷網路狀態是否正常。

5.5.6.2.2 收集防火牆之 log，並統計 log 資料。

5.5.6.2.3 監控內部網路頻寬使用狀況，於頻寬使用率達 60%以上時，應評估增加頻寬之必要性。

5.5.6.3 異常監控作業

5.5.6.3.1 定期監控各伺服器提供之各項服務是否正常，若設備服務狀態不正常時，應通知相關負責人員處理。

5.5.6.4 異常處理作業

5.5.6.4.1 以節點方式由內而外檢測，由回應數值推知問題點。

5.5.6.4.2 確認與問題點相關之實體設備和網路線是否正常。

5.5.6.4.3 如為設備問題可尋找替用設備更換，並連絡廠商維修，並將處理情形記錄於「異常事件紀錄表」。

5.5.7 網路入侵之處理

5.5.7.1 網路被入侵時，應依「安全事件管理程序書」辦理。

5.5.7.2 應建立網路入侵事件之調查程序，除利用工具及稽核檔案提供之資料外，應協請相關單位（如網路服務提供者），追蹤入侵者。

5.5.7.3 入侵者之行為若觸犯法律規定，構成犯罪事實，應立即告知相關單位，請其處理入侵者之犯罪事實調查。

5.6 電子郵件安全管理

5.6.1 電子信箱帳號之註冊、離職、異動申請，應遵循電子郵件相關管理規範之規定，除學生帳號由本校批次建立外，其餘則填寫「電子郵件帳號申請表」提出申請，經各單位部門主管核准後，再交由系統管理者或經授權之管理者建置相關資料。

5.6.2 應建立電子郵件之安全管理機制，以降低電子郵件可能帶來之業務

上及安全上之風險。

5.6.3 應禁止發送匿名信，或偽造他人名義發送電子郵件騷擾他人，導致其他使用者之不安與不便。

5.6.4 敏感等級（含）以上的資料或文件，應避免以電子郵件傳送。

5.6.5 不得傳遞大量且非必要的資訊，避免網路壅塞及資源浪費。

5.6.6 電子郵件附加之檔案，應事前檢視內容有無錯誤後方可傳送。

5.6.7 對來路不明之電子郵件，不宜隨意打開電子郵件，以免啟動惡意執行檔，使網路系統遭到破壞。

5.6.8 郵件伺服器異常處理及故障排除作業

5.6.8.1 發現郵件伺服器系統異常，資訊人員應進行診斷，辨識異常原因及影響範圍，評估系統回復時間，並進行排除作業。

5.6.8.2 異常處理人員應定時回報權責主管最新狀況及處理進度。

5.6.8.3 如異常發生無法立即排除故障時，應通知相關部門異常影響程度及預估回復時間，並採取因應措施。

5.6.8.4 如診斷可能係硬體設備故障造成，則通知廠商人員到場檢測。

5.6.8.5 系統經復原並確實檢查測試後，終止緊急應變作業，並通知相關部門及主管。

5.6.8.6 將處理過程及結果記錄於「異常事件紀錄表」中。

5.7 全球資訊網（WWW）

5.7.1 對 HTTP 伺服器開放可存取的範圍，應限制僅能存取資訊系統之某一特定區域之功能與權限，HTTP 伺服器應透過組態的設定，使其啟動時不具備系統管理者身分。

5.7.2 公告之資訊，應經由權責管理人員之審查與核定，確認未含機密性或敏感性的資訊、違反本系統資訊安全管理之相關資訊，以及違反智慧財產權或法令所明定禁止之資訊。

5.7.3 開放外界連線作業之資訊系統，應避免外界直接進入資訊系統或資料庫存取資料。

5.7.4 內部使用的瀏覽器，對下載之檔案應設定掃描是否隱藏電腦病毒或惡意內容。

5.7.5 當伺服器執行之應用程式需接收自使用者回傳資料時，應予嚴密監控，以防止不法者利用來執行系統指令，獲取系統內重要的資訊或破壞系統。

5.8 電腦管理及安全防護

5.8.1 系統負責人應定時檢查作業系統及硬體設備之效能，並注意作業系統版本更新及問題資訊，做最適建議及導入。

5.8.2 主機負責人應進行伺服器主機監控，檢查系統、安全及應用程式日誌紀錄、或其它有關之系統狀況。一旦發現任何問題得請相關人員協同處理，必要時並通知廠商處理。

5.8.3 為提升伺服器主機連線作業之安全性，應視需要使用加密通道（如VPN、SSH）等各種安全控管技術。

5.8.4 應關閉不需要之服務。

5.8.5 系統負責人需定期檢視更新系統安全修補、防毒軟體及防毒碼，以維持系統正常運作。

5.8.6 應保存稽核紀錄，並定期審查。

5.8.7 系統負責人應於每工作日上班時依「巡查紀錄表」所列項目檢查各主機狀況，以確保系統正常運作。

5.8.8 軟體由系統負責人安裝，安裝時應視狀況通知相關技術人員支援或通知使用者，以避免資訊服務中斷或影響業務。

5.8.9 系統軟體測試由系統負責人辦理，測試時應事先公告並通知及協調相關人員支援，且視狀況需要通知相關人員及使用者以避免因資訊

服務中斷而影響業務。

5.8.10 異常狀況排除

5.8.10.1 遇異常狀況時系統負責人應先行回報資訊安全官，視需要採適當方式處理。

5.8.10.2 通知本校相關人員協助，並說明詳細原因、先行處理步驟及相關資料。如無法自行排除則向維護廠商報修維護，並將故障情形公告及通知使用者及相關人員。

5.8.10.3 將處理過程及結果記錄於「異常事件紀錄表」中。

5.8.11 系統入侵之處理

5.8.11.1 立即拒絕入侵者任何存取動作(例如關閉可疑帳號)，以防止災害繼續擴大。

5.8.11.2 關閉受侵害的主機，並立即與網路離線。

5.8.11.3 檢查防火牆及系統紀錄，研判入侵管道之方式，必要時作安全漏洞修補。

5.8.11.4 通知主機供應商提供必要的回復協助。

5.8.11.5 如伺服主機的完整性受侵害，應將完整的系統備份資料存回受害主機上，並測試其功能，直至完全回復止，最後再將該主機重新上線。

5.8.11.6 將處理過程及結果記錄於「異常事件紀錄表」中。

5.9 可攜式電腦儲存媒體管理

5.9.1 系統資料若需以可攜式媒體保存時，該媒體應存放於安全設備或處所。

5.9.2 儲存媒體所使用之密碼或編碼技術不應透露予遞送人員或與業務無關之人員。

5.9.3 儲存媒體遞送前應加以妥善包裝保護，避免發生實體損壞。

5.9.4 儲存媒體如委由外部單位（例如：郵局或快遞公司）運送，應選擇具有信譽之廠商，並採取以下控制措施：

5.9.4.1 放置於上鎖之容器或以彌封方式處理。

5.9.4.2 當面送達並簽收。

5.9.4.3 資料內容應使用密碼保護。

5.9.5 該儲存媒體之報廢，請詳「資訊資產異動作業說明書」，且須經核准。

5.10 資料備份

5.10.1 各項系統設定檔、伺服器檔案及資料庫資料均應由各系統負責人員訂定備份週期，並依據週期執行系統排程或手動備份，備份狀況應記錄於「備份狀況紀錄表」。

5.10.2 應定期於測試主機上測試備份復原是否正確。

5.10.3 重要系統資料應考量建立異地備份機制。

5.11 安全稽核事項

5.11.1 對各項系統視需要留存系統最新參數設定檔。

5.11.2 系統管理、技術諮詢與機房操作人員工作應依職務與相關規定確實記錄其工作內容於「巡查紀錄表」內。

5.11.3 每月應檢視一次各設備中系統時間是否一致，並進行校正及同步作業。

5.11.4 系統稽核資料應依系統重要性進行備份保護作業，並由專人定期審核，系統管理者不得新增、刪除或修改稽核資料，審查週期不得超過 6 個月。

5.11.5 應定期查核技術符合性，進行弱點掃描或滲透測試，以確定資訊系統及網路環境符合安全實施標準。掃描週期如下：

5.11.5.1 每半年至少針對伺服器及網管設備執行一次。

5.11.5.2 當系統有重大變動時。

5.11.5.3 新系統上線前。

5.11.6 系統異常及安全事件記錄與分析，依據「矯正及預防管理程序書」辦理。

5.11.7 弱點掃瞄報告與修補作業

5.11.7.1 執行弱點掃描應產出弱點掃描報告，弱點掃描報告格式不拘，惟應包含下列內容：

5.11.7.1.1 弱點掃描檢測範圍。

5.11.7.1.2 弱點掃描檢測時程。

5.11.7.1.3 弱點風險等級說明。

5.11.7.1.4 安全弱點列表與建議修補措施。

5.11.7.2 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。

5.11.7.3 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。

5.11.8 殘餘弱點管理

5.11.8.1 弱點若因故無法修補，應於「弱點處理報告單」說明無法修補之原因與防禦因應方法。

6 相關文件

6.1 資訊安全政策

6.2 委外管理程序書

6.3 系統開發與維護程序書

6.4 安全事件管理程序書

6.5 資訊資產異動作業說明書

6.6 矯正及預防管理程序書

6.7 巡查紀錄表

6.8 防火牆進出規則申請表

6.9 備份狀況紀錄表

6.10 異常事件紀錄表

6.11 電子郵件帳號申請表

6.12 弱點處理報告單