南開科技大學系統安全管理辦法

壹、目的

為維持南開科技大學（以下簡稱本校）及確保資訊系統之正常運作，規範管理人員維護系統運作與資料之安全性的作法，程式委外開發及維護及委外廠商管理，特訂定「南開科技大學系統安全管理辦法」(以下簡稱本辦法)。

貳、依據

一、南開科技大學資訊安全政策。

二、南開科技大學資訊安全實施綱領。

三、南開科技大學資訊安全營運持續計畫。

四、國際資訊安全標準 2013 年版(ISO/IEC 27001:2013)。

五、國際資訊安全作業規範 2013 年版(ISO/IEC 27002:2013)。

參、作業存取控制管理

一、電腦帳號管理

(一)本校教職員工登錄校務行政系統以及電子郵件之帳號與密碼，皆由人事資料自動產生。學生電子郵件帳號依學生學號建立，密碼於首次登入時由使用者自行建立。學生電子郵件帳號依學生學號建立，密碼於首次登入時由使用者自行建立。

(二)使用者帳號名稱不得附帶有足以辨識使用者權限的資訊。

(三)各系統中只允許必要之帳號存在，非必要之帳號應予刪除，屬匿名(anonymous)帳號一定要取消其登入之權限。

(四)各系統負責人應每半年至少清查一次使用者帳號，確保使用者帳號資料之正確性與保留必要性，辦理帳號取消、停用或權限調整，清查的結果應送圖書資訊服務處處長審核。

二、系統維護帳號管理

系統軟體與硬體維護廠商因承接本校維護計畫，需要登入本校資訊系統時，得於合約簽訂並簽署保密切結書後，填寫「南開科技大學資訊系統外部使用者帳號申請單」向圖書資訊服務處系統發展組或網路服務組申請系統維護專用帳號，該帳號不得具有主機系統特許權限。

三、系統特許權限帳號管理

(一)應嚴格管控系統之特別權限，定期檢查擁有權限之人員，並將系統特別權限授權資料建檔，作為日後之查考依據。

(二)系統的特許權限帳號（administrator、root、資料庫管理者等系統軟體管理者帳號之權限）應每半年至少清查一次，清查的結果應送圖書資訊服務處處長審核。

四、自動離線的保護

本校校務行政系統及 webmail 網頁服務，應設定自動離線。對於資訊機房內之伺服器主機，則限定於資訊機房內操作並以畫面鎖定保護。

五、連線作業時間的限制

本校因應教職員生上網作業之需求，不限定線上登錄連線時間。

肆、資訊安全管理

一、安全性監控

資訊機房之監控包含網路效能、主機事件、資料庫事件、網路事件、安全攻擊事件、溫溼度、UPS 電力、資訊機房 DVR、資訊機房門禁系統及各相關主機、網路設備之監控，系統監控與稽核軌跡(log trail)之稽查至少應每季定期執行，並留下稽查記錄，作為資訊安全管理系統有效性查核之證據及日後查考之用途。系統監控與稽核軌跡(log trail)之稽查應包括下列項目：

(一)使用者帳號系統登入的記錄，確定使用者帳號是否有不正常使用的情形。

(二)系統特許權限帳號使用的情形及配置情形。

(三)系統存取失敗情形。

(四)例外事件及資訊安全事項的稽核記錄。

二、系統軟體安裝管理

(一)主機系統中所啟動的應用服務，如非必要，不得以主機管理者(Administrator)或超級使用者(root)權限的帳號來執行，降低應用系統被入侵的風險。

(二)主機系統負責人員於安裝系統軟體或應用軟體時，應僅針對必要使用之部分進行安裝，主機系統則應僅啟動必要之服務。

(三)新建置或安裝之軟體，安裝完成後應立即更新廠商預設之密碼。

(四)系統公用程式應進行安全管控，其機制為：

1.應嚴格限制及控制電腦公用程式之安裝與使用。

2.設定使用者通行碼以保護系統公用程式。

3.將有權使用系統公用程式的人數限制到最小的數目。

4.移除非必要的公用程式及系統軟體。

三、作業安全管理

(一)主機管理人員應評估主機系統中各系統軟體與應用軟體的修補程式是處於最新的狀態。

(二)系統管理人員未經權責主管人員許可，不得閱覽、增加、刪除或修改其他使用者上傳之私人檔案。如發現有可疑之網路安全情事（如病毒或特洛依木馬等），系統管理人員得使用適當的工具追蹤檢查相關檔案，如確定為感染病毒，為避免病毒擴散，得經圖書資訊服務處網路服務組組長同意後，逕行掃毒或隔離檔案並知會該檔案擁

有者。

(三)應建置系統開發與測試環境，俾與提供服務之作業環境區隔，避免因系統軟體或應用軟體之開發及測試影響作業環境安全防護之運作。

(四)主機管理人員將主機系統鐘訊同步於同一來源。

(五)主機應避免明碼儲存機敏資料，應施以適當之加密技術，以確保資料安全。

(六)電腦主機應保持桌面淨空，螢幕保護應設於 10 分鐘(含)以內，並以密碼保護。

四、電腦病毒及惡意軟體之防範

(一)病毒防護軟體由本校圖書資訊服務處統一進行規劃評估與建置。

(二)資訊機房網段建置有資料庫之重要微軟視窗平台應設置入侵偵測系統，網路管理人員應隨時監控非法入侵之行為，並收集入侵證據作為法律控訴之證物。

(三)本校教職員生應使用合法具版權軟體，避免交換使用或上網下載來路不明之軟體、資料。

伍、系統變更

一、重大系統變更審查及授權執行作業如下：

(一)人員非經授權不得執行調整或變更網路、主機及其硬體設備環境位置之服務架構。

(二)重大系統變更前，需先進行完整的資料備份並確實測試所有的系統，以確保系統變更作業不會影響原有的安全控制措施與其他系統之正常運作。與外部交換資料時，使用資料前應先啟動病毒防護軟體偵測。

(三)執行系統變更前，須完成填寫「南開科技大學資訊系統變更申請單」。

二、應用系統版本升級或變更作業，應注意事項如下：

(一)非經授權不得執行應用系統版本升級作業，項目包含：變更原廠系統軟體套件版本或服務程式套件。

(二)對於程式原始碼修改或系統軟體套件之更新應有適當之原始碼版本控制或系統軟體套件控管。

(三)應用程式開發或維護時，須經過申請並留下審核紀錄。

三、軟體更新前應保留舊版，以作為緊急應變及回復作業之用。

四、本校教職員生應不定期注意病毒防護資訊，隨時下載病毒碼更新與下載修補系統漏洞。

五、操作電腦系統如發現病毒時應立即清除，無法自行清除病毒時通知圖書資訊服務處網路服務組協助處理。

陸、可攜式設備管理

一、可攜式電腦管理

內部使用之可攜式電腦必應遵守下列事項：

(一)應安裝防毒軟體並啟動主動更新，以保持病毒碼為最新狀態。

(二)不得安裝與業務無關的軟體（包含非法軟體與來路不明之軟體）。

(三)若需與外部其他電腦（或攜帶型儲存設備）交換資料時，應先經過掃毒。

(四)應隨時更新修補程式。

二、可攜式儲存媒體管理

(一)本校員工得使用可攜式儲存媒體備份儲存個人工作資訊。

(二)嚴禁將機密性及敏感性資料儲存至個人系統或儲存媒體，如有特殊業務需求，應經單位主管同意後始得為之。

(三)如有個人業務相關的機密性及敏感性資訊儲存至可攜式儲存媒體時，應予以加密或設定密碼保護處理，不得提供直接儲存於媒體中讀取，避免意外遺失或遭有心人士竊取。

三、攜出設備之安全管理

(一)電腦（包含伺服器主機、桌上型個人電腦、可攜式電腦）攜出校外使用時，應啟動個人系統防火牆功能，應避免非必要連結網路。

(二)電腦借用攜出人員應負保管之責，妥善使用及保管電腦。

(三)電腦攜出使用不得任意安裝或下載軟體使用。

(四)電腦攜出使用完畢歸還時，管理人員應進行防毒檢查，降低本校遭受攻擊的風險。

柒、網路管理

一、網路存取管制

(一)網路區隔防護

為管制網路存取，於資訊機房對外存取節點均應設置防火牆或代理伺服器，對伺服器的存取須透過防火牆管制，強制區隔安全防護網段及各個不安全的網段，並限制網際網路的存取方式。

(二)路由存取路徑管制

為達到資訊安全管理系統執行的要求，路由存取路徑的管制應留有相關紀錄，對每一個防火牆開放的服務均保留一份申請紀錄，服務類別如為公用網路系統的需求而開放的服務，由圖書資訊服務處網路服務組網路管理人員填寫申請單，因各應用系統的需求而開放的服務，由相關人員填寫申請單，經圖書資訊服務處網路服務組組長同意後開放，申請單如「南開科技大學網路服務連結申請單」。

(三)路由存取路徑使用管理與權限審核

1.網路服務連結申請經審核通過後，申請人應定期注意使用期間(時

段）之必要性，遇有系統續用、調整、停用或使用屆期時，應依程序申請網路服務續用、調整或撤銷。

2.對於限期之網路服務連結申請單應採列管措施，遇有屆期或逾期者，則逕關閉網路服務，不另行通知。

3.對於職務異動或業務內容變動者，應主動檢討其申請或使用之網路服務，查有非必要對其開放之網路服務時，應通知後取消該網路服務。

(四)診斷埠保護

本校設置於資訊機房之伺服主機及網路設備，圖書資訊服務處對資訊機房之實體安全機制及相關設備的訊息監看(Diagnostic)或管理設定(Console)埠，應妥善保護其連結之安全性，相關辦法參見本校「南開科技大學資訊機房管理辦法」。

(五)實體連結的限制

本校資訊機房內保護網段的網路中介設備(Switch)應採取嚴格的管控機制，所有非使用中的連結埠應採不提供連結服務，如確有擴增需求，由圖書資訊服務處網路服務組另行連結。

(六)無線網路存取

本校建置之無線區域網路系統，為配合教育部「校園無線漫遊機制整合實驗與推廣計畫」，除提供本校教職員生以 Email 帳號、通行碼登入存取外，亦提供參與漫遊機關學校人員使用個人之 Email 帳號、通行碼登入使用。

為防護本校資訊安全管理系統實施範圍的安全，圖書資訊服務處資訊機房內禁止未經申請使用無線區域網路存取。

(七)外部存取

本校教職員工或維護廠商如因業務特殊需求，應於防火牆對外開放特殊服務（如遠端登入或檔案傳輸等），在不影響本校網路安全條件下（如採用 VPN tunnel、SSH 技術），得提出「南開科技大學網路服務連結申請單」經圖書資訊服務處網路服務組組長核可後設定防火牆權限開放。

外部存取服務應盡量避免常時性的開放，如有迫切的作業需求，應以電話聯繫確認後作暫時性開放，使用結束後即予以關閉，並依程序補填「南開科技大學網路服務連結申請單」。

二、網路服務的安全

為管理本校網路服務的安全性，防火牆與伺服器僅開放必要之服務設定，其他非必要的服務一律阻絕；以達到網路服務的安全。

(一)所有教職員生使用的網路服務安全

為考量校園開放學習環境，未制定相關辦法，進行管制在校教師、職員與學生所使用之網路協定及服務。

(二)系統管理之安全

機房主機系統安全管理，結合防火牆、SSL-VPN 與對外部開放之跳板主機，以提昇機房主機安全管理措施。

三、網路管理系統

為方便管理本校網路,圖書資訊服務處應建置一套網路管理系統進行相關工作。網路管理系統應具備以下功能：

(一)應能對每個網路端點 IP 進行流量管理，必要時得進行阻斷其通訊。

(二)網路異常狀態必應能以 Email 或簡訊通知管理人員。

(三)可以記錄網路端點 IP 異常的狀態，並提供查詢及報表列印功能。

四、網路管理者的責任

(一)網路管理人員應負責建立及維護本校網路系統使用者帳號，並記錄網路系統異常狀況及相關維護書面資料。定時統計本校網路使用情形，及網路設備現況評估，以提高網路速率，及作為擴充設備之憑據，如發現異常狀況應依緊急應變處理程序處理。

(二)網路管理人員未經權責主管人員許可，不得閱覽、增加、刪除或修改其他網路使用者之私人檔案。

(三)網路管理人員登入主機或網路系統時應保留所有登出入系統紀錄，不得新增、刪除或修改稽核資料檔案，避免於安全事件發生後造成追蹤查詢之困擾。

(四)網路管理人員應定期檢查及撤銷閒置不用的帳號，並不得將其重新配賦給其他的使用者。此外，並應確認移除非必要的帳號存在（如 anonymous…等）。

(五)每位網路使用者僅得核發一個使用者帳號，如有特殊情形（如系統測試、免費軟體下載等用途），得經簽奉各所屬單位主管核定，並送圖書資訊服務處網路服務組組長核可後，始得建立帳號。

(六)網路管理人員應隨時注意監控網路的運作，如遇安全事件，應即時啟動緊急應變處理程序。

捌、委外廠商的管理

任何與本校簽署正式協議之機關與廠商委派人員提供本校服務，或本校因應政府法規或行政命令採用外部單位提供的服務，本校應對提供服務的委外廠商進行適當的管理。與本校無正式協議之外部單位，本校不得使用其所提供的服務（公共服務除外）。

一、協議委外廠商的服務內容安全性審查。

二、委外廠商人員的資格審查。

三、委外廠商人員的保密切結書。

四、每年應執行委外廠商現場實地訪查，審查紀錄需文件化經主管查核，列入會議審查與討論。

五、委外廠商提供之服務變更時，應正式函文通知並經雙方同意後始得進行變更。

玖、資訊系統委外開發或維護。

一、需求單位應提出系統開發需求，由圖資處委由承包廠商進行開發或維護。

二、資訊系統開發或維護應與廠商議定保留文件資訊。

三、資訊系統安全需求分析應考量事項如下：

(一)應遵守法規對資訊安全控制的要求。

(二)評估保護資訊機密性、完整性及可用性的需求：

1.對具關鍵或敏感的資訊，應在傳輸或儲存過程中予以加密保護，以確保其機密性。

2.對關鍵或敏感的資訊若有需要，應在傳輸或儲存過程中使用數位簽章或訊息鑑別碼，以偵測訊息內容是否遭受未授權的更改或破壞，確保訊息的完整性與可鑑別性。

四、圖資處同仁應與需求單位確認需求可行性，若需求可行，通知相關維護廠商進行開發或維護。若需求不可行，應由圖資處同仁與廠商及需求單位同仁溝通後，將該需求退回單位。

五、廠商於資訊系統開發或維護完成後，由圖資處同仁先行測試，若功能符合，再轉交需求單位測試。

六、圖資處同仁將原始碼標示版本並且結案歸檔。

壹拾、系統安全稽核

一、稽核監控系統與事件紀錄管理

(一)網路與安全監控系統

應設置防火牆及網管系統對網路事件進行監控，並應定期檢視相關紀錄以達到監控的目標。

(二)主機稽核系統

系統管理人員登入重要主機系統時應保留所有登出入系統紀錄，不得新增、刪除或修改稽核資料檔案，避免於安全事件發生後造成查詢事件軌跡之困擾。

另為保護稽核日誌的獨立完整性，應將所有 UNIX like 主機及 Windows 等重要主機的相關稽核日誌，包含系統紀錄(syslog)、訊息紀錄(message)與事件紀錄(eventlog)等集中管制，並定期檢視重要主機所記錄的軌跡。

二、系統弱點掃瞄

為強化資訊系統的安全，降低系統軟體被已揭露的漏洞或是應用軟體留下的後門，甚或是不當引入的木馬程式對本校造成安全的危機，定期的系統弱點掃瞄是一種適當的防護手段。

(一)弱點掃瞄的方法與策略

1.在內部對所有主機及網路設備進行檢測

此種掃描方式不需透過防火牆，因此可以檢查出所有弱點掃描工具可辨識的安全弱點。

掃瞄的策略為：每半年至少應掃瞄一次，掃瞄結果應與前次比對，以判定漏洞修補之有效性。

2.從 Internet 對暴露在外的主機及網路設備進行檢測

此種掃描方式應包括防火牆內部網段，其範圍與外部惡意攻擊者所能接觸到的範圍一樣，可以檢測出實際暴露在 Internet 可能被利用的弱點。本校視專業必要性委託廠商執行此項掃瞄。

(二)弱點掃瞄的後續處理

1.弱點掃瞄結果初步分析

弱點掃描報表應按風險高低分類，並針對不同的區域進行風險加權的考量，做為漏洞修補優先順序之重要參考依據。

2.漏洞修補評估

辦理漏洞修補前，應與各相關系統負責人討論初步掃描分析結果，評估漏洞修補之影響範圍、修補方法，施作時程等，並完成掃瞄報告與修補建議。

修補的建議方式可為更新 patch、關閉服務狀態、更新軟體版本、限制服務提供目標…等方法，另於評估過程亦應確認弱點是否為誤判，必要時得以人工進行檢視。

3.系統漏洞修補

針對高風險弱點項目，應個別擬定預訂修補期限，並責成相關人員於限期內完成修補工作。

4.修補成效分析

對於掃瞄分析的結果、修補的結果、修補的時效性，以及各次弱點的分佈及關連性應做整個弱點管理的成效分析報告，藉由此成效報告進行整個弱點修補的有效性管理。

壹拾壹、輸出紀錄

一、南開科技大學資訊系統外部使用者帳號申請單(編號：SM01)

二、南開科技大學網路服務連結申請單(編號：SM02)

三、南開科技大學資訊系統變更申請單(編號：SM03)

四、南開科技大學委外廠商遠端連線作業紀錄表(編號：SM04)

五、南開科技大學委外廠商資通安全檢查表(編號：SM05)

壹拾貳、系統安全管理辦法之修訂

本辦法經「資訊安全管理委員會」會議審議通過，陳請校長核定後公告實施。

修訂時亦同。

附件一：

南開科技大學系統安全管理辦法項目對照表

項次	規範要項	參照 ISO/IEC 27001:2013 項目
參	作業存取控制管理	A.9.1.1、A.9.1.2、A.9.2.1、A.9.2.2、A.9.2.3、A.9.2.4、A.9.2.5 與 A.11.2.9。
肆	資訊安全管理	A.9.4.1、A.9.4.2、A.9.4.5、A.10.1.1、A.12.4.1、A.12.4.2、A.12.4.3、A.12.4.4、A.12.6.2、A.12.7.1 與 A.12.2.1。
伍	系統變更	A.12.1.1、A.12.1.2、A.12.5.1 與 A.12.2.1。
陸	可攜式設備管理	A.6.2.1、A.12.2.1、A.12.6.1 與 A.12.6.2。
柒	網路管理	A.13.1.3、A.13.1.1、A.13.1.2、A.13.2.1、A.13.2.2、A.13.2.3 與 A.13.2.4。
捌	第三方服務的管理	A.15.1.1、A.15.1.2、A.15.1.3、A.13.2.3、A.15.2.1 與 A.15.2.2。
玖	系統安全稽核	A.12.7.1 與 A.12.6.1。

第 1.0 版 97 年 6 月 20 日資訊安全管理委員會會議審議通過

第 1.01 版 97 年 6 月 24 日校務會議通過

第 1.1 版 97 年 7 月 23 日資訊安全管理委員會會議審議通過

第 1.2 版 98 年 6 月 8 日資訊安全管理委員會會議審議通過

第 1.3 版 100 年 9 月 13 日資訊安全管理委員會會議審議通過

第 1.4 版 101 年 09 月 03 日資訊安全管理委員會會議審議通過

第 1.5 版 102 年 05 月 31 日資訊安全管理委員會會議審議通過

第 2.0 版 103 年 11 月 27 日資訊安全管理委員會會議審議通過

第 2.1 版 104 年 6 月 4 日資訊安全管理委員會會議審議通過

第 2.11 版 104 年 9 月 1 日資訊安全管理委員會會議審議通過