管理系統文件

文件類別	第二階文件	
文件編號	ISMS-P-012	
文件名稱	網路安全管理程序書	
發行單位	文件管制小組	
發行日期	111 年 02 月 17 日	
版　次	2.4	
訂修廢單位	審　查	核　准
資通安全處理小組		

（原版簽名頁保存於資通安全處理小組）

訂　　修　　廢　　記　　錄		
版次	發行日期	訂 修 廢 內 容 摘 要
2.0	104/04/30	2015 改版發行。
2.1	105/04/01	修訂發行。
2.2	107/03/09	修改本文件防火牆連線服務異動申請單、資訊設備重大弱點補強紀錄表保存地點資訊科技中心單位名稱為圖書資訊處。
2.3	108/04/15	因應資通安全管理法修訂本文件
2.4	111/02/17	新增 5.2.9.4~5.2.9.7 金鑰管理程序。

1. 目的

為使本校網路安全之管理有一明確規範，以確保資料透過網路進行傳輸時之安全性，並透過程序化之安全控管機制，以防止未經授權的系統存取，使網路正常運作，特制定本程序書。

2. 適用範圍

本校所有連接內部網路及對外網路之設備及相關人員的網路管理，均適用本程序書。

3. 參考文件

3.1. 資通安全責任等級分級辦法

3.2. ISMS-W-002 一般資通設備安全管理作業標準書。

3.3. ISMS-P-013 帳號密碼及存取控制管理程序書。

3.4. ISMS-P-018 委外作業管理程序書。

3.5. ISMS-P-009 資通安全事件通報及應變管理程序書。

3.6. ISMS-P-015 資訊備份管理程序書。

3.7. ISMS-P-014 系統發展與維護管理程序書。

3.8. ISMS-P-008 矯正及預防管理程序書。

3.9. ISMS-P-003 資訊資產管理程序書。

3.10. ISMS-P-016 資通設備維護與管理程序書。

4. 名詞定義

4.1. 網路使用者

指經過適當授權並具有使用網路資源之人員。

4.2. 網路系統管理人員

確保網路資源之安全管理，並維護其機密性、完整性與可用性。

4.3. 系統管理者

負責維運與管理所管轄之伺服器主機系統，並確保伺服主機系統提供正常之服務。

4.4. 權責主管

負責核准相關網路設備使用及連線之申請，並督導網路設備之安全管理。

4.5. 防毒軟體

安裝於前端使用者（Client）電腦中，具有病毒過濾及防護功能之系統。

4.6. 惡意程式

4.6.1. 病毒

病毒是一段電腦程式碼，它會將自身附加到程式或檔案，在電腦之間傳佈，並在散佈途中感染電腦。病毒可能會損壞使用者的作業系統、軟體、硬體和檔案。

4.6.2. 特洛伊木馬程式

特洛伊木馬程式不像電腦病毒一樣會感染其他檔案，特洛伊木馬程式通常都會以一些特殊管道進入使用者的電腦系統中，然後伺機執行其惡意行為（如竊取或刪除檔案、竊取密碼等）。

4.6.3. 電腦蠕蟲

蠕蟲（Worm）就像病毒，會透過掌控電腦上可傳輸檔案或資訊的功能自動進行複製。例如蠕蟲可將它本身的複本傳給電子郵件通訊錄所列出的每個人，該人員的電腦接著會執行相同的動作，從而發生大量網路流量之連鎖效應，進而降低整個網路和網際網路的速度。當新的蠕蟲散播時，它們會以極快的速度散佈開來，塞滿網路並可能讓使用者等待兩倍的時間才能檢視網際網路上的網頁。

4.6.4. 間諜程式

間諜程式並非病毒或惡意的程式碼，而是危及隱私的應用程式，允許駭客在使用者毫無知覺的情況下取得電腦的控制權。它們經常隨著使用者下載想要的應用程式的同時，不知不覺地下載到使用者的電腦上。這些安全威脅包括間諜程式、廣告軟體、惡意撥號程式、惡作劇程式、駭客工具、遠端存取工具、密碼破解應用程式，以及其他未分類的軟體。

4.7. 重大惡意程式感染事件

4.7.1. 大範圍個人電腦或伺服器主機系統遭受病毒感染。

4.7.2. 因中毒造成大規模網路癱瘓。

4.8. 弱點

指軟硬體資通設備上，已揭露且可被利用進行攻擊之技術漏洞。重大弱點為弱點發布單位或系統原廠所定義之嚴重、重大或應立即改善之弱點，應考量本校的防禦強度與相關安控機制，認為技術風險超出可接受範圍，應立刻著手補強。

4.9. 安全性修正程式（Patch）

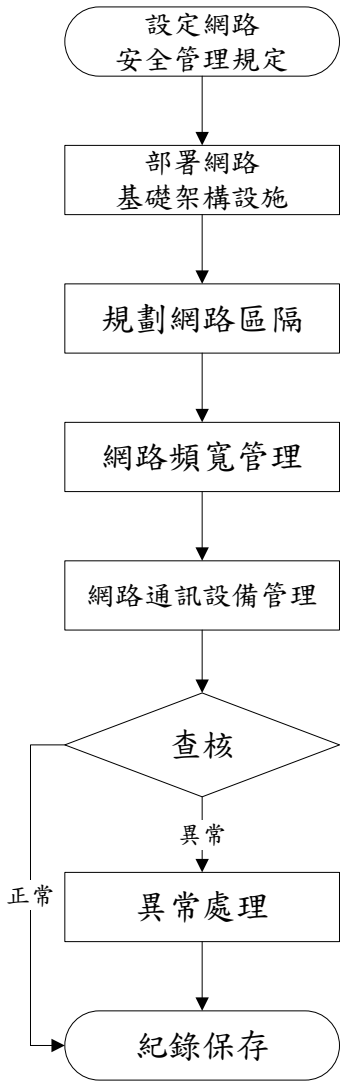
針對特定資通設備技術安全性弱點所廣泛部署的修正程式，其中依據廠商定義與部署方式不同，亦可稱為更新（Update）、修補（Hotfix）或服務套件（Service Pack）等。

4.10. 檢核人員

負責弱點掃描與威脅比對作業，專責檢查各設備之弱點是否依據計畫定期補強。

5. 作業內容

5.1. 網路安全管理流程圖

作業流程	權責單位	相關表單
	資通安全處理小組 網路系統管理人員 系統管理者/資通人員 資通安全處理小組 資通安全處理小組 資通安全處理小組 網路系統管理人員 資通安全處理小組 資通安全處理小組 資通安全處理小組 系統管理者 相關業務承辦人員	防火牆連線服務異動申請單 資通設備重大弱點補強紀錄表 資通安全事件通報單

5.2. 設定網路安全管理規定

5.2.1. 網路使用者安全管理

5.2.1.1. 本校網路須經授權始可使用，已授權的使用者，僅能在授權範圍內存取網路資源。

5.2.1.2. 不得將自己的登入身分識別與密碼交付他人使用。

5.2.1.3. 禁止以任何方法竊取他人的登入身分識別與密碼。

5.2.1.4. 禁止以任何儀器設備或軟體工具竊聽網路上的通訊。

5.2.1.5. 不得以任何手段蓄意干擾或妨害網路的正常運作。

5.2.1.6. 應遵守上述網路安全規定，並確實瞭解其應負的責任，如有違反網路安全情節，依相關法規辦理。

5.2.1.7. 使用瀏覽器應先評估所瀏覽網頁之安全性，並將適度調整瀏覽器安全性設定（如將「網際網路」之安全層級設定為「中」以上）。

5.2.1.8. 有關本校使用網路、電子郵件等之相關規定，請參閱「ISMS-W-002 一般資通設備安全管理作業標準書」。

5.2.1.9. 資通系統使用權限之申請程序應依據「ISMS-P-013 帳號密碼及存取控制管理程序書」之規定辦理。

5.2.2. 網路傳輸及存取控制管理

5.2.2.1. 「密」等級（含）以上資訊未經密碼保護禁止使用公眾網路傳送。

5.2.2.2. 廠商或專案相關外部人員對內部需進行資訊存取作業時，應遵循「ISMS-P-018 委外作業管理程序書」之規範予以控管，避免重要資訊被經由網路外洩。

5.2.2.3. 對於開放提供外部單位存取之服務，必須限制使用者之網路功能以確保網路安全。

5.2.2.4. 網路路由之規劃必須確保任何網路連線或資訊傳輸符合網路存取之安全需求。

5.2.3. 網路服務安全管理

5.2.3.1. 只開放必須的網路服務功能與通訊協定。如需異動，由相關人員進行安全評估，確定可行且無安全上的顧慮後，填寫「ISMS-P-012-01 防火牆連線服務異動申請單」且經權責主管核准後方得開放。

5.2.3.2. 應定期審閱防火牆政策，每年至少一次，相關紀錄應留存備查。

5.2.3.3. 對所有必須開放的網路服務功能與通訊協定應於防火牆安全設施中管制。

5.2.3.4. 網路系統管理人員應配合資通安全政策與規定，隨時檢討及調整網路設備的設定，以反應最新狀況與需求。

5.2.4. 網路防毒安全管理

5.2.4.1. 使用者如需使用外來的可攜式設備或儲存媒體，必須先進行掃毒的動作，以避免電腦、系統與網路受到惡意程式威脅。

5.2.4.2. 本校全體員工應使用由本校所提供之電腦防毒軟體，並安裝於所使用之個人電腦中，自動或定期檢查硬碟及儲存媒體之檔案，確保無電腦病毒潛伏於個人電腦與儲存媒體中。

5.2.4.3. 收取郵件時，若收到來路不明之電子郵件，應立即刪除，並禁止開啟來路不明之檔案或電子郵件及其附加檔案。

5.2.4.4. 系統管理者或個人電腦使用者應將重要資料定期備份。

5.2.4.5. 電子郵件之使用規範，應依據「ISMS-W-002 一般資通設備安全管理作業標準書」之規定辦理。

5.2.4.6. 系統伺服主機須由系統管理者評估其需要，若需要則必須即時安裝防毒軟體。

5.2.4.7. 本校個人電腦應安裝防毒軟體，並定期更新病毒碼及掃毒程式。

5.2.4.8. 各系統伺服主機與個人電腦需由各系統管理者及個人電腦使用者自動與定期執行病毒碼更新作業，並應設定排程自動

執行掃毒作業。

5.2.4.9. 如遇疑似惡意程式感染情況，防毒軟體無法處理或作業仍不正常時，使用者應立即通報資通人員處理；資通人員確認為惡意程式感染事件後，應判斷感染途徑及其惡意程式名稱，並應協助使用者將惡意程式移除或隔離。

5.2.4.10. 當惡意程式無法移除或隔離時，資通人員應立即將電腦關機，並中斷網路連線，如無法短時間內處理，則重新安裝作業系統並利用備份還原資料。

5.2.4.11. 如遇重大惡意程式感染事件，業務承辦人員應依據「ISMS-P-009 資通安全事件通報及應變管理程序書」之規定通報相關人員。

5.2.5. 安全性檢測安全管理

5.2.5.1. 為確保本校各項資通系統能持續提供穩定的服務，必須定期執行安全性檢測作業，預先找出各項資通系統潛在的弱點，並擬定對策執行預防措施，以降低威脅及衝擊所造成的風險。

5.2.5.2. 資通安全處理小組應針對電腦機房重要伺服器主機、網路設備等，依「資通安全責任等級分級辦法」定期辦理安全性檢測作業，並提出安全性檢測報告。

5.2.5.3. 安全性檢測完成後，弱掃人員須將安全弱點記錄於「ISMS-P-012-02 資通設備重大弱點補強紀錄表」中，交付各系統管理者，由各系統管理者自行或視需要取得委外服務廠商之協助，以確認弱點是否確實存在。

5.2.5.4. 針對安全性檢測報告，應親自或委由專業服務廠商，於重大弱點發現或公布時，立即進行威脅比對作業，以判別弱點與威脅是否已造成資通安全事件，若造成資安事件則依據「ISMS-P-009 資通安全事件通報及應變管理程序書」之規定辦理各項資安事件通報與處理。

5.2.5.5. 對於可取得相關廠商提供安全性修補程式之弱點，得依循下列作業進行修復與測試。

5.2.5.5.1. 系統管理者應自行或委由廠商依據所知悉之弱點，進行弱點補強作業，並將補強結果記錄於「ISMS-P-012-02 資通設備重大弱點補強紀錄表」中。

5.2.5.5.2. 於修補弱點前應進行技術風險評估，並依據弱點影響性、資產重要性及弱點修復作業的可行性（例如評估部署對於網路服務效能的影響、對於停機或重新開機時間的影響等），以進行修補優先次序規劃。

5.2.5.5.3. 弱點修補人員應確認安全性修補程式的來源及可靠性，避免自不明網站或郵件中下載取得。

5.2.5.5.4. 對於重大之弱點，系統管理者須於弱點公告或安全性檢測報告提出後盡速完成修補作業或提供其他足以降低弱點風險的控制方法。

5.2.5.5.5. 安全性檢測報告產出後，檢核人員須立即以系統區分將安全弱點列表並交付各系統管理者，由系統管理者或委外廠商對所負責之系統主機進行弱點修補作業。

5.2.5.5.6. 系統管理者接到所負責系統主機之安全弱點列表後，須立即檢視弱點是否確實存在，並視需要取得委外服務廠商之協助進行弱點修補作業。

5.2.5.5.7. 系統管理者需進行安全性修補程式部署前之規劃準備，包含確認部署的範圍、安全性修補程式的相依性與部署順序，及可否合併部署以減少系統重新啟動之衝擊等。

5.2.5.5.8. 安全性修補程式部署前，亦應考慮復原程序，包括確認是否可以解除安裝部署、安排必要的程序以防電腦在部署修補程式後停止回應，以及進行適當的資料或系統備份及還原程序等。備份作業應依據「ISMS-P-015 資訊備份管理程序書」之規定辦理。

5.2.5.5.9. 系統管理者須盡可能將安全程式部署的嚴重性、緊急性及潛在的負面影響告知業務相關人員。

5.2.5.5.10. 若進行修補之標的為重要之線上系統時，於正式部署作業前，盡可能於相似的環境進行接受度測試，以確認安

全性修補程式可以在正式作業環境中正確運作。

5.2.5.5.11. 部署時之相關變更注意事項，依據「ISMS-P-014 系統發展與維護管理程序書」之變更管理相關章節辦理。

5.2.5.5.12. 於部署作業完成後，系統管理者應檢閱變更內容。包括查看相關設備之事件及系統紀錄檔，找出安全性修正程式部署之成功或失敗等相關資訊。必要時，得使用弱點掃描報告來監視更新部署狀況。

5.2.5.6. 殘餘弱點之安全管理作業

5.2.5.6.1. 系統弱點若因故無法成功修補，系統管理者須依據修補作業實際情形，將無法補強的原因以及因應控制措施，詳實記錄於「ISMS-P-012-02 資通設備重大弱點補強紀錄表」以利後續追蹤控管。

5.2.5.6.2. 對於修補作業後仍有殘餘重大弱點之重要設備，應說明其他因應措施以降低弱點風險，並將此結果記錄於「ISMS-P-012-02 資通設備重大弱點補強紀錄表」中備查。

5.2.5.6.3. 弱點掃描人員應利用弱點掃描報告之統計結果，分析弱點改善之狀況，並於會議中提出檢討。弱點若無法限期處理及改善，則依據「ISMS-P-008 矯正及預防管理程序書」之相關規定執行矯正與預防措施，進行問題矯正及風險預防的作業。

5.2.6. 網路入侵偵測安全管理

5.2.6.1. 應於網路入口處，部署網路入侵防護系統，進行入侵偵測與防護。

5.2.6.2. 網路系統管理人員應配合資通安全政策及規定，隨時檢討及調整網路入侵系統的設定，以反應最新的狀況與需求。

5.2.7. 佈線安全管理

5.2.7.1. 網路通訊設備於安裝時，應注意機房之電力線路架構，應執行網電線路區隔，以防相互干擾。

5.2.7.2. 易遭受破壞之線路設施應妥善保護(如光纖),以免因其他工程裝設而影響網路之運作。

5.2.7.3. 線路應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。

5.2.7.4. 線路配置需注意維護安全與方便，應避免糾結與裸露。線路如需異動，須經由專責人員執行。

5.2.8. 網路相關紀錄與蒐證安全管理

5.2.8.1. 內、外部網路管理人員進行網路維護作業後，應使用相對應之表單以建立相關紀錄，作為日後稽核與蒐證之依據。

5.2.8.2. 網路管理人員應定期檢視網路存取之紀錄，並留存查核紀錄。

5.2.9. 網際網路應用系統之安全

5.2.9.1. 為保護網際網路上傳輸而涉及應用服務的資訊，免於詐欺行為、契約爭議及未經授權的揭露與修改，網路管理人員應定期執行弱點掃描或滲透測試服務，並將其技術脆弱點進行修補，以確保重要資訊之機密性及完整性。

5.2.9.2. 網際網路應用系統所提供各項服務之資訊，若涉及機密資料時應啟動安全之加密防護機制(如：VPN、SSL 等),確保資料安全及未經授權的揭露與修改。

5.2.9.3. 網際網路應用系統若須進行系統變更作業時，應依「ISMS-P-014 系統發展與維護管理程序書」之相關規定提出申請及審核，確保應用系統變更受到適切之監督及管制。

5.2.9.4. 密碼（Key）原則或策略可考量以下因素：

5.2.9.4.1. 使用密碼管控制組織之範圍及受保護之相關業務資訊（含行動裝置）。

5.2.9.4.2. 加密演算法之強度與保護級別應納入風險評估。

5.2.9.4.3. 加密密鑰的保護、遺失、洩露或可能之損壞管理作法。

5.2.9.4.4. 密碼策略應考慮到法規和國家限制等適用之可能性。

5.2.9.4.5. 密碼控制應納入實現不同的資通安全目標之考量。

5.2.9.5. 若採購憑證機構所發行之公鑰憑證，則該機構宜為聲名卓著之組織，備妥適當之控制措施及程序，提供所要求之信賴程度。

5.2.9.6. 憑證資料應於「ISMS-P-03-01 資訊資產清冊」中登錄，並評估資產價值及進行風險考量，檔案應妥適保存。

5.2.9.7. 於網際網路有提供服務之應用系統伺服器，至少每年須檢查憑證效期一次；過期或無效的憑證應進行銷毀，避免誤用或造成損害。

5.3. 設置網路通訊基礎架構

本校網路通訊基礎架構（Network Infrastructure）之設置、維護及更新，由資通安全處理小組負責規劃，並呈送權責主管及相關單位審核後安裝建置。

5.4. 規劃網路區隔

規劃適當網路區隔之管理機制，以防止不當網路存取行為與流量散佈。

5.4.1. 內部網路之使用，應對使用狀況與條件區分不同網路區段，以便進行網路存取控管，各區段應以特定的安全設施（如：防火牆及網路閘門）加以保護，以降低可能的安全風險。

5.4.2. 內部網路之使用，應鑑別主機與使用者之工作內容，並賦予適當網路區段之 IP 位址，以供網路存取控制管理考量。

5.4.3. 對外網際網路服務與內部網路使用需求應設定適當存取控制機制，防止機密性資訊外洩。

5.4.4. 非經授權嚴禁使用無線網路及私有有線設備與網路介接。

5.5. 網路頻寬管理

5.5.1. 配置相關管理系統以進行網路流量之監控，並執行紀錄，保障網路頻寬之正常使用。

5.5.2. 禁止網路使用者將網路資源使用於私人用途。

5.5.3. 網路系統管理人員如發現網路流量異常，應立即分析網路異常原因並採取適當之矯正措施，並將結果記錄於「ISMS-P-009-01 資通安全事件通報單」中備查。

5.6. 網路通訊設備管理

5.6.1. 確保網路通訊設備之機密性、完整性及可用性，應依據「ISMS-P-003 資訊資產管理程序書」之規定予以控管。

5.6.2. 網路通訊設備之維護改善，應留有紀錄備查。

5.6.3. 網路通訊設備於安裝上線前，應進行安全與作業影響評估，並考慮是否請廠商提供到場協助，做為第二線技術支援。

5.6.4. 廠商到場進行網路設備安裝、維護工作時，應派員全程陪同監控。

5.6.5. 廠商之維護方式以到場服務為原則。但若有實際需要需做遠端連線測試時，須依據「ISMS-P-018 委外作業管理程序書」之規定予以控管。

5.6.6. 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。

5.6.7. 為維持網路持續正常運作，各重要網路通訊設備應規定委外維護廠商於契約規定時間內修復，或以備品更換。

5.6.8. 重要網路通訊設備應透過不斷電系統提供電力，以達穩壓及防止不正常的跳電狀況。

5.6.9. 網路通訊設備應由專人負責維護故障叫修之相關工作，並紀錄維護狀況。

5.6.10. 網路通訊設備之維護管理作業，應依據「ISMS-P-016 資通設備維護與管理程序書」之規定辦理。

5.7. 異常處理

經查核結果若發生異常，由系統管理者依據「ISMS-P-008 矯正及預防管理程序書」之相關規定執行矯正與預防措施，進行問題矯正及風險預防的作業。

5.8. 紀錄保存

相關業務承辦人員應參照如下規範，妥善保存各項紀錄。

編號	表單名稱	保存地點	保存期限
1	防火牆連線服務異動申請單	圖書資訊處	至少 1 年
2	資通設備重大弱點補強紀錄表	圖書資訊處	至少 1 年

6. 附件

6.1. ISMS-P-012-01 防火牆連線服務異動申請單。

6.2. ISMS-P-012-02 資通設備重大弱點補強紀錄表。

6.3. ISMS-P-009-01 資通安全事件通報單。

開　南　大　學
K A I N A N　U n i v e r s i t y

防火牆連線服務異動申請單

申請日期		服務啟用期間	自　年　月　日至　年　月　日止	
欲連線設備名稱(內部)			欲連線設備IP(目的端)	
連線用途				
使用軟體或協定(必填)			使用埠號（必填）	
外部連線 IP (來源端)				
校方申請人資料	姓　名		電　話	
	E-Mail			
申請廠商負責人（請加蓋公司大小章）	姓　名		電　話	
	地　址			
	公司章		負責人章	

以下連線單位免填

承辦人		權責主管審核	

（審核後填寫）

防火牆設定新增/異動紀錄

規則編號	動作	來源端物件名稱	目的端物件名稱	設定人員與日期	說明
	□新增 □異動				

說明事項	※申請人願意遵循以下說明事項。 1.外單位欲連線本資訊處設備一律使用本申請表格 2.欲連線資訊設備請小心操作。若設備因不當操作所引起系統故障、損毀，則由申請連線單位修復或賠償。 3.請校方申請人員務須要求所屬廠商，配合本校資訊安全政策的各項規定。 4.其他未盡事宜，請依照圖書資訊處管理人員之說明。

開南大學
KAINAN University

資通設備重大弱點補強紀錄表

系統名稱：		填表日期：　　年　　月　　日
內部 IP：	外部 IP：	掃描時間：　　年　　月　　日
弱點總數：	已修正弱點數：	未修正弱點數：

※ 風險等級共分成「高」、「中」、「低」三級，風險等級請依實際情況填寫，風險等級「高」者須優先處理。

No	弱點名稱	風險等級	修正作業說明	最近嘗試修正日期	無法補強原因與因應措施	修正人員