管理系統文件

文件類別	第三階文件	
文件編號	ISMS-W-002	
文件名稱	一般資通設備安全管理作業標準書	
發行單位	文件管制小組	
發行日期	108 年 04 月 15 日	
版次	2.1	
訂修廢單位	審查	核准
資通安全處理小組		

（原版簽名頁保存於文件管制小組）

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	108/04/15	因應資通安全管理法修訂本文件

1. 目的

為促使本校職員在使用一般資通設備（如：個人電腦、可攜式設備、可攜式儲存媒體等）及各項網路服務（如：www、電子郵件等）時有一明確之規範，避免一般資通設備因人為疏失、蓄意竊取或不當使用，導致資通安全遭受危害、個人資料外洩等情事，降低因濫用、誤用所造成的資安風險及強化本校資通安全管理，特制訂本標準書。

2. 適用範圍

凡本校職員對個人電腦、可攜式資通設備、可攜式儲存媒體、印表機、掃描器等一般資通設備及各項網路服務之使用與管理，均適用本標準書。

3. 參考文件

3.1. ISMS-P-003 資訊資產管理程序書。

4. 名詞定義

4.1. 可攜式資通設備

包含筆記型電腦、平板電腦、智慧型手機、個人數位助理（PDA）、數位播放器、數位相機、錄音筆、燒錄設備或其他具存取數位資料功能之可攜式資通設備及其周邊設備等。

4.2. 可攜式儲存媒體

可供使用者透過資通設備之通信埠，如 Ethernet、USB 埠、1394 埠等進行大量資料存取之媒體，包含 USB 隨身碟、可攜式硬碟、磁片、光碟片、Compact Flash（CF 卡）、Secure Digital card（SD 卡）等數位相機記憶卡或其他具存取數位資料功能之媒體。

4.3. 一般資通設備

意指桌上型個人電腦、可攜式資通設備、可攜式儲存媒體、印表機、影印機、傳真機及掃描器等一般性資通設備。

5. 作業內容

5.1. 一般使用規範

5.1.1. 本校所配發之一般資通設備以公務使用為原則。資訊單位協助個人電腦合法版權軟體之安裝，使用者須合理的使用個人電腦資源，且符合本校使用規範並接受相關稽查管考。

5.1.2. 個人電腦、筆記型電腦或平板電腦等應依正常開（關）機操作程序使用及保管，下班或長時間不用時應關機並關閉相關電源，可攜式儲存媒體應上鎖保護。

5.1.3. 離開座位時，應將電腦鎖定及啟用螢幕保護程式，並啟動密碼以保護電腦資料安全，並將螢幕保護啟動時間設定在 10 分鐘以內，以避免他人偷窺及使用電腦。

5.1.4. 管制區內個人電腦不得使用無線網路（如 Wi-Fi、藍芽等）或行動通訊網路連接至外部網路環境。

5.1.5. 筆記型電腦及平板電腦等須攜出使用時，請妥善保管，且應先評估外部網路環境之安全性，不可隨意連線至不明或不安全之無線或有線網路環境。

5.1.6. 個人電腦之軟、硬體安裝後，使用者在使用時如發生任何問題，應立即向負責人員反應處理。

5.1.7. 使用者之個人電腦應隨時保持清潔，每季至少擦拭外觀一次。

5.1.8. 電腦使用者嚴禁擅自拆卸或加裝電腦週邊設備或更改系統環境設定（如 IP、GATEWAY、DNS 等）。

5.1.9. 電腦須啟用作業系統內建之個人防火牆功能。

5.1.10. 存放於一般資通設備之機密性檔案非經核可不得攜出，且應加密或設密碼保護，以防止資料外洩。

5.1.11. 因業務需要須開啟網路芳鄰分享檔案時，應將存放機密資料的資料夾或是檔案本身加密或是加密碼保護，以確保資料存取之安全性。

5.1.12. 如遇疑似惡意程式或病毒感染情況，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。

5.1.13. 個人電腦使用者應定期將重要之資料進行備份。

5.2. 網路連線使用規範

5.2.1. 一般規範

5.2.1.1. 使用者需經授權並賦予相關存取權限後，始得使用本校所提供之各項網路服務，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. 使用者不得將個人之網路登入身分識別與密碼交付他人使用，亦禁止以任何方法竊取他人的登入身分識別與密碼。

5.2.1.3. 禁止以任何儀器設備或軟體工具竊聽網路上的通訊，也不得以任何手段，蓄意干擾或妨害網路的正常運作。

5.2.1.4. 使用者如發現網路出現異樣時，應立即將電腦關閉或將網路斷線，並通報專責人員處理。

5.2.1.5. 嚴禁利用本校網路散布機密性或違反法令法規之資料及檔案。

5.2.1.6. 禁止瀏覽不當之網站（如暴力、色情、賭博、惡意網站等），並不得使用與工作無關之串流媒體、MP3、圖片、檔案等傳輸，以避免造成網路壅塞。

5.2.1.7. 禁止使用點對點（Peer to Peer, P2P）類型的傳輸軟體（如ezPeer、KURO、FOXY、e-Donkey、BT…等類型軟體）下載檔案及提供檔案分享。

5.2.1.8. 除因公務需要且經權責主管核可外，禁止傳送機密性資料檔案給他人或傳送至網際網路上（如他人之郵件信箱或個人外部郵件信箱、網路硬碟、雲端儲存空間、FTP 站及即時通訊軟體之傳送等）。

5.2.1.9. 使用民間業者提供之雲端儲存空間（如：Google、Dropbox等）、FTP 站台及個人外部郵件信箱等，應避免傳輸公務資料（含機敏資訊），以免造成本校相關資訊外洩；如屬個人產製之資料，亦應使用加密工具，以避免個人隱私資訊洩漏。

5.2.1.10. 電腦須啟用作業系統內建之個人防火牆功能，電腦使用者應定期將重要之資料進行備份。

5.2.1.11. 因業務需要須開啟網路芳鄰分享檔案時，應將存放機密資料的資料夾或是檔案本身加密或是加密碼保護，以確保資料存

取之安全。

5.2.2. 智慧財產權

5.2.2.1. 禁止下載或安裝來路不明、非公務使用及有違反法令疑慮（如智慧財產權等）的資訊檔案、電腦程式與軟體，以防止被植入後門或木馬程式。若需安裝軟體，須取得合法授權後，始可進行相關作業。

5.2.2.2. 未經著作權人之同意，使用者不得將受保護的著作上傳於公開之網站上。

5.2.2.3. 使用者不得利用本校網路進行其他可能涉及侵害智慧財產權之行為。

5.2.3. 網路安全

5.2.3.1. 使用瀏覽器應先評估所瀏覽網頁之安全性，並適度調整瀏覽器安全性設定（如設定「網際網路」之安全層級為「中」以上）。

5.2.3.2. 機密性資訊未經加密或啟動密碼保護，一律禁止使用公眾網路進行傳送。

5.2.3.3. 使用者不得將色情檔案建置在本校網路，亦不得在網路上散播色情文字、圖片、影像、聲音等不法或不當的資訊。

5.2.3.4. 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。

5.3. 電腦防毒及惡意軟體入侵保護管理

5.3.1. 本校個人電腦應安裝防毒軟體，電腦使用者或管理者應注意病毒碼更新狀況並定期執行個人電腦、筆記型電腦病毒掃描。本校電腦所安裝之防毒軟體，不得擅自卸載或移除。

5.3.2. 與其他外部電腦、可攜式資通設備及可攜式儲存媒體交換檔案資料時，必須先經過病毒掃描方可進行。

5.3.3. 電腦使用者或管理者應定期更新作業系統及其它應用程式之弱點修補程式，並保持更新至最新狀態。

5.3.4. 如遇疑似惡意程式或病毒感染情況，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單位人員處理。

5.4. 帳號密碼使用規範

5.4.1. 使用者於第一次登錄系統時，應立即更改預設密碼，並妥善保管帳號與維持密碼之機密性。

5.4.2. 密碼長度設定
一般資通設備使用者之密碼長度設定至少 8 碼（含）以上，且須每隔 6 個月更換密碼一次，密碼變更時應避免重複或循環使用舊密碼。

5.4.3. 密碼內容設置原則

5.4.3.1. 密碼內容之設定，應包含阿拉伯數字及英文字母，建議包含特殊符號。另重要資通系統（如：網域及含有個人資料等系統）的密碼建議採複雜性原則。

5.4.3.2. 複雜性原則
密碼必須包含英文大寫字母、英文小寫字母、阿拉伯數字及特殊符號四個類別中至少兩種。

5.4.3.3. 密碼內容之設定，避免使用與個人有關之資料做為密碼，如下說明：

5.4.3.3.1. 使用者識別碼、出生年月日、身分證字號。

5.4.3.3.2. 汽機車牌照號碼、機關單位簡稱。

5.4.3.3.3. 電腦主機名稱、作業系統名稱。

5.4.3.3.4. 電話號碼、空白、字典字彙（具有意義的英文單字，例如：flower、eagle、birthday 等）。

5.4.4. 使用者須負密碼保護之責，不得對任何人透露或以任何形式公開自己帳號及密碼，以避免密碼外洩。

5.4.5. 本校人員及委外廠商有保護通行碼之責，應避免將帳號、密碼記錄在書面上或張貼在個人電腦、終端機螢幕或其他未保護且容易洩漏秘密之處所。

5.4.6. 各系統之密碼嚴禁轉知他人，使用者若懷疑其密碼被他人知悉或發現密碼可能遭破解時，應立即更改密碼。

5.4.7. 禁止使用者與他人共用自己或他人的帳號及密碼，且帳號與密碼應存放於安全之處，保存帳號、密碼之檔案應以加密或加密碼之方式保護。

5.4.8. 禁止盜用或冒用他人帳號及密碼使用網路資源，或將個人帳號及密碼借予他人使用。

5.4.9. 使用者忘記密碼時，應依帳號及密碼申請規定向系統管理者提出申請，由系統管理者確認身分後，重新設定新密碼。

5.4.10. 使用者每次存取系統時應輸入密碼登入系統，避免使用記錄密碼功能，導致開機時自動登入系統。

5.5. 電子郵件使用規範

5.5.1. 一般規範

5.5.1.1. 電子郵件使用者需經授權並賦予相關存取權限後，始得使用本校電子郵件系統收發電子郵件。

5.5.1.2. 為避免遭他人冒用個人電子郵件信箱，使用者應妥善保管密碼且定期更改密碼，並不得將個人帳號借予他人使用。

5.5.1.3. 禁止使用帳號傳送或轉發煽動性、毀謗性、威脅性、猥褻性、商業性及違法的電子郵件。

5.5.1.4. 內部互傳或對外的每封電子郵件傳送時，不應超過規定之大小限制，並禁止傳送垃圾郵件，以免影響頻寬，浪費網路資源。

5.5.1.5. 禁止電子郵件使用者發送電子郵件騷擾他人，或偽造他人名義發送電子郵件，導致其他使用者之不安與不便。

5.5.1.6. 禁止開啟或轉寄來路不明的電子郵件及其附件檔案或連結，以免遭受惡意程式或病毒的感染。

5.5.1.7. 非公務需求且未經權責長官核可，禁止透過電子郵件寄送未加密或未啟用密碼保護之機密性資料，且勿將密碼寫在

E-mail 內容中。

5.5.1.8. 經權責長官核可後若使用電子郵件傳送機密等級屬「機敏」之文件資料，應於傳送之前設定密碼保護。

5.5.1.9. 若公務需要需透過電子郵件傳送機密檔案時，需經權責長官核可，並將檔案加密碼保護或以適當的加密或電子簽章等安全技術處理。

5.5.1.10. 郵件收發軟體應設定純文字閱覽信件，關閉郵件預覽及不自動下載 HTML 郵件中的圖片功能，並取消自動回條功能。

5.5.2. 智慧財產權

5.5.2.1. 不得引用來源不明的電子郵件或檔案內容。

5.5.2.2. 禁止以電子郵件傳遞或交換非法之應用軟體。

5.5.3. 網路安全

5.5.3.1. 禁止隨意開啟來路不明之電子郵件，以避免惡意程式或病毒感染。

5.5.3.2. 電子郵件使用者如發現疑似電子郵件病毒事件，應立即關閉個人之電子郵件收發軟體，並通報專責人員處理。

5.6. 可攜式設備及儲存媒體之使用規範

5.6.1. 員工一律禁用可攜式設備及可攜式儲存媒體等設施，如公務上須使用則須提出申請經權責主管核准後方可使用。

5.6.2. 可攜式設備及可攜式儲存媒體僅限於公務使用，禁止使用於私人用途，使用時應僅防資訊外洩或中毒。

5.6.3. 使用可攜式儲存媒體時須先進行掃毒以確認其不含病毒與惡意程式，掃毒後方可進行資料之上傳及寫入作業。

5.6.4. 將機密資料存放於可攜式儲存媒體上時，得採取適當加密處理或設定密碼保護（如 Word、Excel 或壓縮軟體之密碼功能），避免可攜式儲存媒體遺失時造成資訊外洩。

5.6.5. 筆記型電腦應安裝防毒軟體，並定期檢查作業系統修正程式與更

新病毒碼為最新版本。

5.6.6. 存有重要機密性資訊之可攜式資通設備或儲存媒體攜出時，設備管理人員應負保護之責不得離身，且針對相關檔案資料須執行加密或先清除其機密資訊，以避免資料洩露，另作業完成後須徹底抹去媒體上相關資料。

5.6.7. 廠商所交付本校之光碟（含程式、系統文書、手冊或其他業務資料等），其保存應由專人保管。

5.6.8. 筆記型電腦於本校外部環境使用時，應考量以下防護措施：

5.6.8.1. 筆記型電腦須於本校外部環境使用網路時，應先評估網路環境之安全性，並確認電腦內之防毒軟體已更新為最新版本。

5.6.8.2. 筆記型電腦須於本校外部公共空間使用時，若螢幕畫面顯示敏感或機密資訊時，應注意畫面是否有遭旁人窺視之疑慮。

5.6.8.3. 不可將筆記型電腦置於視線以外之處，應隨身攜帶確保實體安全。

5.6.9. 用外來的可攜式設備及可攜式儲存媒體，必須先進行掃毒的動作，以避免本校電腦、系統與網路受到病毒威脅。

5.6.10. 可攜式設備及儲存媒體遺失時應立即通報單位主管，並評估資料遺失是否具有機密性，依情節之重大程度決定是否向上呈報。

5.6.11. 非本校人員所擁有之可攜式資通設備使用要求：

5.6.11.1. 非本校之可攜式資通設備原則上不得連接本校網路，如須於本校進行軟體開發、測試、示範或電腦作業，限於特定場所使用，且所使用的網段須與本校網路隔離。

5.6.11.2. 非本校人員因特殊需求，須使用其可攜式資通設備進行本校網路連接時，本校相關業務承辦人必須填寫「ISMS-W-002-01 外部人員資通設備網路連接申請單」，並說明連接本校網路需求用途。

5.6.11.3. 連接本校網路之可攜式資通設備須具備適當之防毒能力，並更新至最新之病毒碼，作業系統及相關應用程式等亦須更新至最新之弱點修正程式。

5.6.11.4. 於本校網路使用可攜式資通設備應遵守本校相關管理規範，不可再開啟其他無線網路裝置，未經申請核可，禁止執行封包、收集分析等軟體以及任何網路偵測之行為。

5.6.11.5. 如上述該項作業之目的為執行網路偵測或封包收集分析，應由本校相關人員全程陪同。

5.6.11.6. 具有照相或錄影功能之可攜式資通設備，未經同意不得進行拍攝，如經本校同意拍攝時應有本校人員陪同。

5.6.11.7. 非本校人員欲使用可攜式儲存媒體攜出本校資料時，本校相關業務承辦人必須填寫「ISMS-W-002-02 外部人員使用可攜式儲存媒體資料攜出申請單」，詳細記載使用人員之服務單位等相關資訊並說明用途，經業務承辦人員確認可攜式儲存媒體不含病毒與惡意程式，方可進行資料上傳及寫入作業，且業務承辦人員應陪同並確認寫入資料之內容。

5.6.11.8. 機密資料檔案的讀取及複製須符合本校各業務單位的規定，並經該單位主管或其授權人員核可。

5.6.12. 燒錄機與光碟片使用管理

5.6.12.1. 安裝燒錄機之主機須具有密碼與作業系統保護，並置於安全之辦公區域。

5.6.12.2. 燒錄完成後之媒體應依「ISMS-P-003 資訊資產管理程序書」按其機密等級進行安全控管。

5.7. 辦公設施之使用要求

5.7.1. 電話管理要求

5.7.1.1. 於開放空間、公共環境使用電話通訊設備時，應避免談論本校敏感性資訊。

5.7.1.2. 用電話時，應留意身邊人員，以防止業務機密資料被竊聽。

5.7.2. 印表機、影印機及傳真機管理要求

5.7.2.1. 列印、影印或傳真機密性文件後，應立即將文件取走，並予以適當保存。

5.7.2.2. 無人領取之資料，若無人認領則於次一工作日執行銷毀。

5.8. 資料保護管理

5.8.1. 除非必要，避免在網站留存個人檔案資料，且盡量不要同意網站使用個人資料在其他用途及分享。

5.8.2. 在網際網路註冊或輸入個人資料時，應注意該單位或網站的公信度、隱私權保護政策、資料是否加密等，並做好相關「隱私設定」。

5.8.3. 重要資料應定期進行備份，且備份後應驗證備份是否成功。

5.8.4. 本校資通設備（含可攜式資通設備及儲存媒體等）送修、汰換或報廢前，應先由使用者確實清除機密性資料檔案，且相關設備、裝置及媒體報廢前，使用者應先做好必要資料之備份工作，由權責單位實施相關儲存資料之消磁或安全性覆寫或實體破壞等措施，使資料不復存在。

5.8.5. 本校人員應落實辦公桌面/螢幕淨空政策，以避免機敏（或含個人資料）文件或光碟等資料遭未經授權使用、遺失或破壞。

5.8.6. 本校同仁離職時，除必要之業務交接資料外，應將相關非必要留存之機敏文件及資料（含自身之個人資料）確實清除。

5.9. 本校同仁因違反本規範而造成資安事件及個資外洩事件，本校得視危害情節輕重簽奉資通安全長核可後，送考績委員會審議懲處。

5.10. 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	外部人員資通設備網路連接申請單	資網中心	至少一年
2	外部人員使用可攜式儲存媒體資料攜出申請單	資網中心	至少一年

6. 附件

6.1. ISMS-W-002-01 外部人員資通設備網路連接申請單。

6.2. ISMS-W-002-02 外部人員使用可攜式儲存媒體資料攜出申請單。

紀錄編號：ISMS-W-002-01-_____-___

開　南　大　學
KAINAN University

外部人員資通設備網路連接申請單

申請單位 填寫資料	申請日期：　　年　　月　　日 申請單位：_____ 申請人：_____　員工編號：_____　電話：_____ 申請起迄時間：　年　月　日　時　分 ～　年　月　日　時　分
外部單位 填寫資料	服務單位：_____ 姓　　名：_____　職稱：_____　電話：_____
使用設備	1. ☐ PC　　型號：_____ ☐ NB　　型號：_____ ☐其他：_____　型號：_____ 2. 作業系統版本：_____ 防毒軟體版本：_____ 網路卡卡號（MAC）：_____　☐已關閉無線網路
用途說明	
使用地點	
申　請　人 檢核項目 (請勾選)	☐非本校人員資通設備已先由本校業務申請人執行設備檢查(內容應包含防毒軟體、作業系統及相關應用程式等須更新至最新之病毒碼、弱點修正程式，且已關閉無線網路裝置)，檢查結果： ☐符　合 ☐不符合　原因：_____ ☐作業之目的為執行網路偵測或封包收集分析，業務申請人員將全程陪同。
承辦單位 審核意見	

申　請　人	申請單位主管
業務承辦人	業務單位主管

開　南　大　學
KAINAN University

外部人員使用可攜式儲存媒體資料攜出申請單

申請單位 填寫資料	申請日期：　年　月　日 申請單位：_____ 申 請 人：_____ 員工編號：_____ 電話：_____ 資料來源設備名稱：_____ IP 位址：_____ 使用起迄時間：年 月 日 時 分 ～ 年 月 日 時 分
外部單位 填寫資料	服務單位：_____ 姓　名：_____ 職稱：_____ 電話：_____
使用種類	1. ☐ USB 隨身碟　型號：_____ ☐可攜式硬碟　型號：_____ ☐記憶卡　型號：_____ ☐其他：_____　型號：_____ 2. ☐須請資訊單位管理員設定相關資料明碼攜出
用途說明	
檔案名稱 (含副檔名) 及內容說明 ※請依序詳細 填列並說明	請勾選： ☐含機敏性資料　☐未含機敏性資料　備註：_____
申　請　人 檢 核 項 目 (請　勾　選)	☐使用之可攜式儲存媒體應先由本校業務申請人執行防毒軟體掃描作業，檢查結果： ☐符　合 ☐不符合　原因：_____ ☐申請寫入之檔案皆已填列及說明 (如檔案過多，請依序列出，附於本申請單後)。 ☐業務申請人員將陪同作業並確認寫入資料之內容。
資訊單位 審核意見	

申　請　人	申請單位主管
資訊單位承辦人	資訊單位主管