敏惠醫護管理專科學校

「資訊安全管理系統」
網路及系統安全管理說明書

機密等級：一般

編　　號：IS-MHCHCM-03-002

版本編號：1.1

制訂日期：112.10.30

使用本文件前，如對版本有疑問，請與修訂者確認最新版次。

本文件歷次變更紀錄：

版次	修訂日	修訂者	說　　明	核准者
1.0	110.12.30	資訊安全執行小組	初版發行	執行秘書
1.1	112.10.30	資訊安全執行小組	修訂頁首、頁尾、作業說明	執行秘書

本程序書由資訊安全執行小組負責維護。

目錄：

1 目的 3

2 適用範圍 3

3 權責 3

4 名詞定義 3

5 作業說明 3

6 相關文件 13

1 目的

1.1 敏惠醫護管理專科學校（以下簡稱本校）的許多營運及核心服務多數都是藉由電腦資訊系統來輔助完成。為了保護這些電腦系統以及其中的資訊，此說明書提供使用本校內電腦系統之所有使用者合適的資訊安全作業說明。

2 適用範圍

2.1 適用於所有獨立作業或是和區域網路或內部網路連接的電腦。

3 權責

3.1 本校內、外部人員均需遵守本說明書。

4 名詞定義

4.1 系統安全 — 安全定義包括伺服器主機、個人電腦、麥金塔電腦、工作站、筆記型電腦、平板電腦、以及其他供個人使用之電腦系統或網路資源，及由系統所處理的資訊。

4.2 業務使用 — 電腦系統或網路資源僅能供本校內各單位所負責的業務使用。

4.3 內部人員 — 任職於本校之人員。

4.4 外部人員 — 非委外廠商及非任職於本校之人員。

5 作業說明

5.1 使用者作業規範：

5.1.1 系統組態及作業變更控制

5.1.1.1 軟體變更：本校內列管使用者能在電腦上執行軟體清單中之軟體。同樣地，使用者不得隨意安裝違反版權之軟體。

5.1.1.2 作業系統變更：使用者得合法變更由本校內所提供之電腦硬體上的作業系統、系統組態設定值、升級既有的作業系統、或者安裝新的作業系統(含虛擬機器 VMware 等)。

5.1.1.3 如果有必要協助變更以上各項設定，則需由資訊單位的相關技術人員協助，協助方式得以親自或遠端操作方式處理。

5.1.1.4 使用者須隨時檢查作業系統漏洞修補通知，或於系統自動更新通知啟動時立即進行系統修補作業。

5.1.2 硬體控制

5.1.2.1 硬體變更：由本校內所提供的電腦硬體設備不得以任何方式加以變更，若因業務上之考量，得事先取得部門主管簽核，再送交資訊單位檢視其硬體變更需求。

5.1.3 存取控制

5.1.3.1 人員至部門報到後填具「資訊系統帳號服務申請單」，經該部門主管簽核，再交由資訊人員核准可開放的相關服務申請。使用者於第一次登入時應立即變更密碼，且必須自行負責其個人密碼的管控。

5.1.3.2 密碼不可使用直接閱讀的形式儲存在批次檔、自動登入檔、軟體的巨集檔案、終端機功能鍵、儲存於未設有存取限制的電腦、或是其他未經授權人士可能看到的地方。

5.1.3.3 密碼設定原則，參照「存取控制管理程序書」中密碼設定原則。

5.1.3.4 使用者離開使用中的電腦時，必須登出。

5.1.3.5 螢幕保護程式應設定於 15 分鐘自動啓動，且設定密碼保護。

5.1.3.6 使用配賦各單位之公用電腦，必須使用個人系統帳號登錄，不得使用他人之系統帳號或共用系統帳號，並於使用完畢後立即登出系統。

5.1.3.7 處理機密資訊的電腦均必須紀錄所有和電腦安全相關的重大事件，且填寫『資通訊安全事件通報單』，並及時通報資訊單位。例如，有人嘗試猜測密碼、嘗試使用未經授權之使用者權限、以及對系統軟體所作出的變更的任何資訊安全事件。

5.1.3.8 外部人員若於服務期間需要使用本校之各項系統服務，必須依以下各項要求取得及使用帳號：

5.1.3.8.1 外部人員若有系統使用之需求，必須填寫「資訊系統帳號服務異動申請單」，經該單位主管簽核，再交由資訊人員核准可開放的相關服務申請。

5.1.3.8.2 外部人員須於「資訊系統帳號服務異動申請單」說明帳號之使用期限。過期之帳號立即停用或刪除，若有延長使用期限之需求，則說明展期期限，並經相關單位主管審核。

5.1.3.8.3 外部人員之系統帳號僅限於在單位內之公用電腦或配賦之電腦使用，不得利用本校內員工的電腦進行系統登錄。

5.1.3.8.4 外部人員於系統帳號使用期間須遵循各系統之使用要求，若有違反使用規定情形，資訊單位得立即停用帳號使用權。並提交單位主管檢討，直至狀況改善後恢復帳號使用權，但須列入管制。

5.1.3.9 校務系統存取管理

5.1.3.9.1 本校校務相關行政人員於報到時經申請單位主管核准後由本中心辦理。

5.1.3.9.2 若有通行密碼遺失時，可透過校務系統進行線上密碼查詢。

5.1.3.9.3 若有權限異動時，需填寫「資訊系統帳號服務異動申請單」，經單位主管及業管單位(系統權責單位)核准後，由系統管理人員進行使用者權限設定作業。

5.1.4　電腦病毒：

5.1.4.1 所有電腦皆應持續執行由資訊單位所提供最新版的病毒偵測程式。使用者不可企圖中斷防毒程式之執行。

5.1.4.2 使用隨身碟、光碟片、或者其他由本校以外的單位所提供之可攜帶式資料儲存媒體，在檢查過無任何病毒之後方可使用。

5.1.4.3 為避免電腦病毒或惡意軟體藉由網路分享傳遞與感染(例如：勒索病毒)，進而影響網路服務安全與運作，所有人員不得任意設定資料夾分享。

5.1.4.4 若檔案為壓縮或加密格式得先(於掃毒用電腦)解壓縮/密，再用病毒檢查程式掃描後，才可以執行。

5.1.4.5 若懷疑電腦已經被電腦病毒或惡意軟體感染，應該盡速的停止使用受感染的電腦及中斷網路連線，並且通知資訊單位。若懷疑電腦病毒或惡意軟體已經開始損害資訊或電腦軟體，應該立即進行關機。

5.1.4.6 使用者不得撰寫、編譯、複製、繁殖、執行、或是嘗試在本校內的電腦上安裝或執行使用任何電腦病毒、蠕蟲、木馬程式或是相關惡意軟體，違者依本校相關規範處理。

5.2 系統管理者作業規範

5.2.1 使用者列冊管理

5.2.1.1 各資訊系統業務使用單位，須填寫「資訊系統帳號服務異動申請單」向資訊單位提出帳號權限申請，並請各系統負責人開立。

5.2.1.2 各資訊系統負責人須對所負責之系統使用人員列冊管理。

5.2.1.3 各資訊系統負責人於受理業務使用人員「資訊系統帳號服務異動申請單」申請時，須遵守下列原則：

5.2.1.3.1 不可重複申請使用該資訊系統之正式授權。

5.2.1.3.2 申請核可後，應以書面、電子或其他方式，告知使用者系統存取權限。

5.2.1.3.3 應建立及維持系統使用者註冊資料紀錄，以備日後查考。

5.2.1.3.4 閒置不用的識別碼，不得重新配賦給其他的使用者。

5.2.2 權限管理

5.2.2.1 特別權限可區分為系統管理員、系統操作員、系統開發或應用程式管理員、資料庫管理員、維護廠商等，其餘皆視為一般權限。

5.2.2.2 各資訊系統負責人應針對使用者業務性質，賦予不同存取權限，並分開造冊管理。

5.2.2.3 對於擁有特別存取權限的使用者，各資訊系統負責人應隨時瞭解記錄其對系統使用情形。

5.2.2.4 系統存取權限之申請及授權資料建檔，以確認責任及預備日後稽核。

5.2.3 系統權限評估

5.2.3.1 為有效控管資料及系統存取，各資訊系統負責人應定期檢討及評估使用者存取權限，並將評估結果填寫於「權限帳號檢視申請紀錄單」。

5.2.3.2 系統存取一般權限評估，以每年評估一次為原則。

5.2.3.3 系統存取特別權限之評估，以每半年評估一次為原則。

5.2.3.4 定期檢討系統存取特別權限核發情形，防止有人未經正式的授權程序取得特別權限。

5.2.4 系統備份與復原作業

5.2.4.1 系統備份與復原作業需遵循本校「資訊備份管理說明書」。

5.3 網路管理

5.3.1 網路管理規範

5.3.1.1 資訊單位為本校網路之管理單位，負責制訂各項網路管理及使用規範，並依規範之要求有效管制本校網路之使用。

5.3.1.2 外部人員若需使用本校網路服務，須填寫「資訊系統帳號服

務異動申請單」，經資訊單位登記核准後始可使用本校網路服務。

5.3.1.3 經過授權的網路使用者必須依本校網路使用規範及教育部「校園網路使用規範」使用網路服務，違反使用規範者得依相關之懲戒規定處理。

5.3.1.4 資訊單位須依以下規定管理本校網路：

5.3.1.4.1 內部人員所需之 IP 位址由資訊單位依其區域網路設定指定配發一組。外部使用者 IP 位址配發亦同。

5.3.1.4.2 為確保資訊與網路安全，資訊單位將隨時監看 IP 位址使用網路服務情形。若發現未經申請程序之電腦或可攜式設備使用本校之網路服務，得立即將其引導至隔離網路區段，不得使用本校網路服務。

5.3.1.4.3 使用網路監控工具監控本校使用網路之狀況，並依以下規定處理違犯規定之網路使用行為：

5.3.1.4.3.1 違反使用規範者，經查證屬實，資訊單位得立即停止其網路使用權，並送交行政會議檢討。並依行為改善狀況，重新啟用其網路使用權，但須列入管制。

5.3.1.4.3.2 使用者使用網路之行為，若觸犯本國相關法律規定者，除立即停止網路使用權外，亦須配合警調單位

調查，由網路使用人負起法律責任。

5.3.1.4.3.3 P2P 點對點傳輸軟體(如：foxy…)禁止使用。

5.3.2 網路使用規範：

5.3.2.1 取得本校網路（含辦公室等網路服務涵蓋區域）使用權之人員，必須依本說明書規範使用網路服務：

5.3.2.2 尊重智慧財產權：網路使用者應尊重智慧財產權，避免下列可能涉侵害智慧財產權之行為：

5.3.2.2.1 使用未經授權之電腦程式。

5.3.2.2.2 違法下載、拷貝受著作權法保護之著作。

5.3.2.2.3 未經著作權人之同意，將受保護的之著作上傳於公開之網站上。

5.3.2.2.4 論壇或其他線上討論區上之文章，經作者明示禁止轉載或未註明可轉載，而仍任意轉載。

5.3.2.2.5 架設網站供公眾違法下載受保護之著作。

5.3.2.2.6 其他可能涉及侵害智慧財產權之行為。

5.3.2.3 禁止濫用網路系統，使用者不得為下列行為：

5.3.2.3.1 散佈電腦病毒或其他干擾或破壞系統機能之程式。

5.3.2.3.2 擅自截取網路傳輸訊息。

5.3.2.3.3 以破解、盜用或冒用他人帳號及密碼等方式，未經受授

權使用網路資源，或無故洩漏他人帳號及密碼。

5.3.2.3.4 無故將帳號借給他人之使用。

5.3.2.3.5 隱藏帳號或使用虛假帳號。但經明確授權得匿名使用者不在此限。

5.3.2.3.6 窺視他人之電子郵件或檔案。

5.3.2.3.7 以任何方式濫用網路資源。包括以電子郵件大量傳送廣告信件、連鎖信或無用信息。或以灌爆信箱、掠奪資源等方式，影響系統之正常運作。以電子郵件、線上談話、論壇或類似功能之方法散布詐欺、毀謗、侮辱、猥褻、非法軟體交易或其他違法之訊息。

5.3.2.3.8 利用本校之網路資源從事與業務無關之活動或違法行為。

5.4 無線區域網路

5.4.1 為確保資訊傳輸的安全，未經授權連線本校內網的無線網路設備不得使用。

5.5 FTP(檔案傳輸服務)服務使用規定

5.5.1 FTP 服務只限於服務本校或因應本校營運相關業務需求所使用。

5.5.2 禁止上傳非法檔案（例如：色情、暴力、賭博、非授權軟體/資

料檔…等）

5.6 遠端存取

5.6.1 若廠商需透過遠端連接本校系統進行維護，需填寫「外對內連線服務申請表」，經主管核准後，由防火牆管理人員進行防火牆規則設定，連線時間依專案合約規範或雙方協議辦理。

6 相關文件

6.1 資訊系統帳號服務異動申請單

6.2 外對內連線服務申請表

6.3 權限帳號檢視申請紀錄單