雙和醫院資訊安全政策

衛生福利部雙和醫院（以下簡稱本院）為強化資訊安全管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供本院之資訊業務持續運作之資訊環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，特定此政策規範。

目標及指標

維護本院資訊資產之機密性、完整性與可用性，並保障使用者資料隱私。藉由全體同仁共同努力來達成下列目標：

1、保護本院業務活動資訊，避免未經授權的存取及修改，確保其正確完整。
2、建立跨部門之資訊安全組織，制訂、推動、實施及評估改進資訊安全管理事項，確保本院具備可供業務持續運作之資訊環境。
3、辦理資訊安全教育訓練，推廣員工資訊安全之意識與強化其對相關責任之認知。
4、執行資訊安全風險評估機制，提升資訊安全管理之有效性與即時性。
5、實施資訊安全內部稽核制度，確保資訊安全管理之落實執行。
6、本院之業務活動執行須符合相關法令或法規之要求。

對資訊安全管理系統有效性貢獻

本院依需要及符合政府與相關法令要求建立資訊安全管理系統。為充份掌握資訊運作及管理過程並滿足各項安全要求與期盼，需要全院同仁共同合作以完善資訊安全管理之有效性。

使用者應遵守事項

一、系統與個人資料管控

1. 針對與本單位重要之系統與個資，應設定相關存取控管機制，及必要之執行或存取紀錄。
2. 各單位所產生之個資紙本及電子檔案資料或紀錄，應妥於保存與管理，以避免其遭受竊取、竄改、毀損、滅失、及洩漏之事件發生。
3. 無論紙本或電子檔案個資，權責單位應善盡資料與檔案之存取控制及管理責任。
4. 每年至少執行 1 次作業系統與應用系統帳號權限清查，清查後應更新帳號權限清單，並刪除不必要之帳號與權限。
5. 相關資料傳輸應在「資料傳輸加密」、「郵件安全控制」及「資料交換安全」之考量或規範下進行。
6. 針對重要資料或個資應建立備份機制。

7. 個資檔案需有專責單位或專責人員負責管理與維護。

二、一般使用者應遵守下列日常作業事項

1. 勿使用他人帳號做任何上線的作業或冒用他人識別資料。
2. 可攜式設備中若含重要資料時，應善盡安全管理責任，應考量將資料加密或對設備上鎖、設定密碼等，避免遺失或遭竊。
3. 使用可攜式儲存設備前，宜進行掃毒，確認無病毒存在。
4. 個人電腦應安裝防毒軟體，病毒碼及修正程式至最妥適版本。
5. 避免經由不明來源或網站下載軟體。
6. 具有螢幕保護程式功能的個人電腦，應啟動螢幕保護程式，並以密碼保護。
7. 違反前述規定經查屬實，且情節重大者，本單位將保留取消其使用之權利，並提報人資或相關單位議處。
8. 本單位禁止使用私人隨身碟，如因業務需要則須向本單位登記取用公用隨身碟，並填「資訊室公用隨身碟借用登記表」，用後歸還及記錄。
9. 個人資料以紙本方式進行傳輸時，應採取彌封或專人遞送，或其他具保密機制之傳遞方式進行。

三、設備管理與控制

1. 電腦、資訊處理設備中，如因業務需求存放機密資訊，應給予適當的保護，例如加密、或設定存取權限，以避免遭未授權之存取。
2. 屬機密類別之資訊不應置放於網路公開之分享區。
3. 以電子郵件或其他電子傳訊方式進行「敏感」或「機密」資訊之傳送時，宜予以加密或以密碼保護後傳送。
4. 電腦存放「敏感」或「機密」資訊者，應定期進行資訊備份，備份後的媒體或檔案應注意其安全防護，以確保資訊之可用性及防止未授權存取。
5. 可攜式媒體(例如外接式硬碟機、USB 隨身碟、智慧型手機…等)，需有相對應知管理或安全防護機制予以管理控制，以確保不被惡意程式入侵，或遭受資料竊取、盜用或滅失。
6. 使用影印機、印表機、傳真機、掃描器或多功能事務機執行個人資料傳輸後，應立即將資料取走。
7. 針對存有個人資料之紙本文件及可攜式媒體，於不使用或下班後，應遵守桌面淨空政策，放置於抽屜或儲櫃並上鎖，以避免外洩。

四、未遵循資訊安全管理系統之可能後果

1. 應確實瞭解並同意遵守本院「資訊安全管理辦法」。任職期間查詢或使用資料庫時，務必為職務所需，且明白均會留下查詢過程及使用狀況記錄。
2. 對於業務上所知悉或持有之資料(含所有文件、圖說、報表、電腦資料、數據等)、程式及其檔案、媒體等，均負有嚴守秘密之義務，絕不洩漏或交付予業務非相關人員，亦不得為自己或第三人利益而使用。
3. 如有違反致發生資料外洩或違法情事時，致本院及所屬員工之權益等遭受

損害時，願負一切法律責任，離職後亦同。