

高雄市新興衛生所

資訊安全政策

| | | |
|-----|----------------|------|
| 第一章 | 前言..... | 3 |
| 第二章 | 資通安全目的..... | 3 |
| 第三章 | 資通安全目標..... | 3 |
| 第四章 | 資訊安全範圍..... | 4 |
| 第五章 | 資安小組職權與架構..... | 4 |
| 第六章 | 政策實施方式..... | 5, 6 |

壹. 前言

資訊化時代的來臨，帶來人民生活的便利，無論在食、衣、住、行方面，有了資訊化的介入，生活資訊的掌控就更顯得快速及明瞭；而資料於電腦中的呈現，也帶來了現代人多元化的選擇及減少文書上費時的往來。

政府資訊化的推動，縮短了公文往返的時間，即時的獲得資料與掌控時效上皆有莫大的助益，但相對的，資料的維護與保密也就相形的重要；『資通安全政策』的擬定也就刻不容緩，其管理程序及安全防護技術應用於各項資訊作業，包括作業執行時工作人員所需遵守的各項原則及程序。鑑於確保資料之彙集、處理、傳送、儲存及流通的安全，本所制定『資通安全政策』以利本所資訊營運的持續性。

貳. 目的

為確保本所資訊機密性、完整性與可用性與防範災變危害所產生的衝擊影響，建立管控程序，降低人為疏失與資料隱密性維護。

參. 目標

強化衛生所資訊安全管理，建立資料之安全與保密並確保資訊業務運作之持續。

肆. 資訊安全範圍

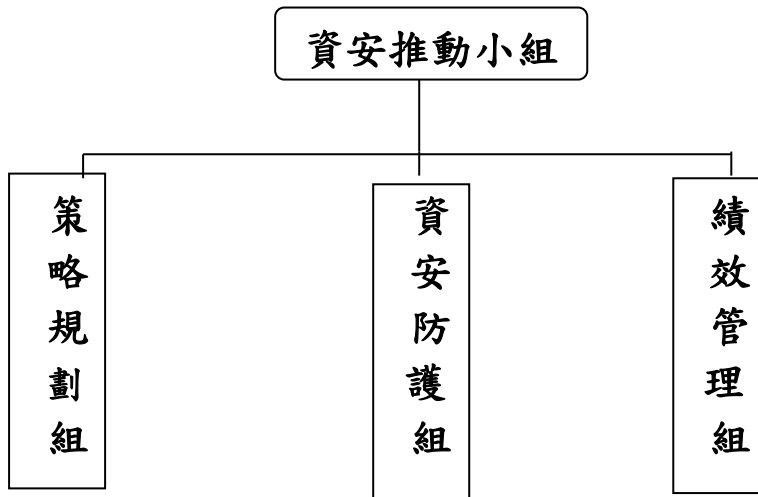
資訊安全管理系統適用範圍包括所有工作同仁與軟、硬體設備，概分類下列：

- 一、 資訊安全權責分工
- 二、 電腦系統安全管理
- 三、 系統存取管制
- 四、 資訊資產安全管理
- 五、 實體及環境安全管理
- 六、 資訓安全稽核
- 七、 人員管理及資訊安全訓練

八、網路安全管理

伍. 資安小組職權與架構

一、組織架構



二、職責

本所資訊安全管理小組由本所所長擔任總召集人，資安推動小組成員則由所長、研考及資訊主辦人與總務人員共同組成，各單位人員權責如下：

I. 策略規劃組：

1. 資通安全政策及目標之研議。
2. 訂定機關資通安全相關規章與程序、制度文件，並確保相關規章與程序、制度合乎法令及契約之要求。
3. 依據資通安全目標擬定機關年度工作計畫。
4. 傳達機關資通安全政策與目標。
5. 其他資通安全事項之規劃。

II. 資安防護組：

1. 資通安全技術之研究、建置及評估相關事項。
2. 資通安全相關規章與程序、制度之執行。
3. 資訊及資通系統之盤點及風險評估。
4. 資料及資通系統之安全防護事項之執行。
5. 資通安全事件之通報及應變機制之執行。
6. 其他資通安全事項之辦理與推動。

III. 績效管理組：

1. 辦理資通安全內部稽核。
2. 每年定期召開資通安全管理審查會議，提報
3. 資通安全事項執行情形。

陸. 政策實施方式

依據 BS-7799-2：2002 指導規範之「規劃-執行-檢查-行動」模式，持續改善資訊安全管理系統。成立「資通安全管理小組」為最高管理階層，以利推動及協調與執行細節。

I. 人員之管理

1. 員工需參加資安訓練並了解資訊安全政策並遵守其規範
2. 訂定系統操作之 SOP，避免使用者操作不當。
3. 離職員工應立即取消各項資訊所有權限，調職或異動也須依系統調整其權限，制定人員異動、離職等之各項資訊申請表單

II. 電腦系統與軟體之安全管理

1. 本所每台電腦需採用密碼制以確保使用者資料保密之安全性

2. 電腦委外修理須與廠商訂定保密合約，以確保資料之機密性
3. 未經許可不得隨意軟體輸入並建立本所軟體使用規範
4. 電腦系統不得隨意遷移位址，如有必要須經資安小組之審視方可執行
5. 防火牆及防毒軟體之建置並隨時更新

III. 系統存取控制

1. 定訂系統存取政策及授權規範，告知員工使用相關權限及責任
2. 建立系統使用者註冊管理制度，加強通行碼管理並定期更新
3. 監視系統存取與使用及記錄並注意電腦時間之同步性

IV. 網路安全管理

1. 開放外界網路連接之網點，應以防火牆及其他安全設施來控管外界與內部網路資料傳輸與存取
2. 機關網站存有個人資料須加強加密保護措施
3. 不得隨意觀看違法之網站，制定網路控管制度

V. 實體及環境安全管理

1. 加強機房進出人員之管控並記錄建立監控系統
2. 建立機房溫度、溼度、電壓之管控及記錄，了解機房之變化情形
3. 不斷電系統之維護

VI. 制定資通安全事件分級管理及通報制度

資通安全事件概分 1、2、3、4 等級；建立資安事件通報手冊及資安人員之名冊與聯絡方式

VII. 確實執行內部稽核管理

每半年定期執行內部稽核作業並紀錄，以持續維護及改善內部資訊作業系統之缺失

VIII. 建立災難復原管理規劃

建立一套作業程序，當電腦遭受中斷時能獲得快速回應能力

1. 建構風險評估及災害影響分析
 2. 設製備份機制或選擇替換設施
- IX. 制定本所資產價值鑑定表、威脅評估表與弱點分析，進而探討本所資訊風險所在
- X. 制定資通安全外部稽核自我審查時之適用性聲明書

I.