資安管理方案及措施

為確保公司在資訊安全做好全方位的管理，擬定三大要件措施如下:

一、資訊安全風險管理架構:

為保障公司及客戶之機密資訊安全，本公司由資訊課負責資訊安全管理與監督，並制定「電子計算機處理作業系統管理辦法」，明定公司機密資訊保護的管理程序及規範，建構全方位的資安防衛能力，並提升員工對資訊安全保護的正確觀念及警覺性，以降低機密資訊外洩的風險。

二、資訊安全政策:

1. 加強資訊系統安全維護：

對外設有防火牆防止有危害資安的病毒入侵；對內購買防毒軟體，加強防範及阻止電腦病毒之襲擊。

2. 資料的保護備援:

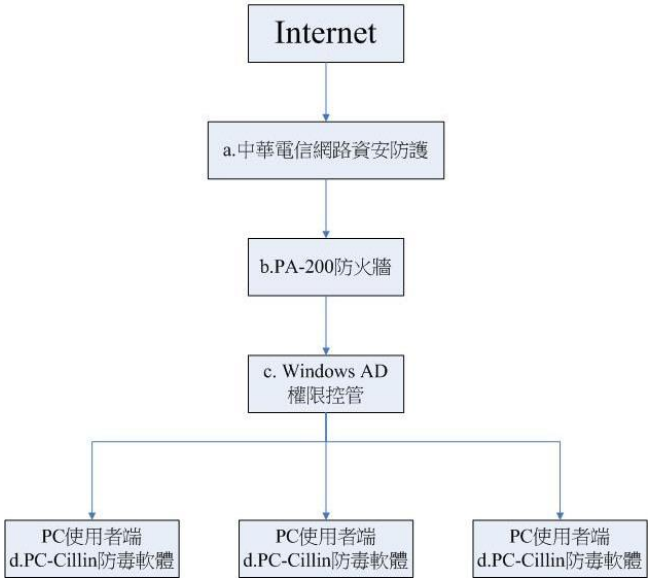
建置備援備份系統，以確保資料遺失後的復原，使電腦作業能迅速恢復，讓資料可安全回復原始內容。

3. 掌握資安新趨勢：

參加資安研討會與廠商交流，並參加資安相關課程之學習，定期關注資安議題並即時規劃因應。

三、資訊安全管理方案:

1. 建置四階層的資料安全防護:防火牆及防毒軟體均自動更新，可以防犯罪新病毒的攻擊。



a. 中華電信網路資安防護:中華電信最新的資安防護，能立即先阻擋病毒進入，以及駭客網站排除。
b. NU840H 防火牆:眾至廠商有建置防駭中心，隨時遠端更新最新的病毒碼及軟體程式至 PA-200 防火牆，這樣能夠 24 小時不間斷保護網路出入的安全。
c. Windows AD 權限控管:使用者要登入系統時，均透過 AD 權限控管，必須輸入帳號及密碼才能進入。
d. PC-Cillin 防毒軟體:公司內部有建立防毒中心，控管所有電腦的防毒軟體，並隨時更新使用者端的電腦病毒碼為最新版，以防止病毒及駭客入侵。

2. 公司人員登入電腦作業均有權限密碼控管，各檔案資料均有嚴格控制帳號的存取權限，只能

存取使用該帳號可用資料。

3. 主機伺服器資料:建置全方位備份資料
   a. 每天系統自動將資料備份至檔案伺服器及磁帶，並於磁帶備份完畢後，由相關人員去取放置於防火保險櫃內。
   b. 建置異地備援系統，每 4 小時更新備援系統資料，如原系統有異常狀況產生時(例如:硬體損壞)，可隨時啟動備援系統，大大提高做到資料的可回復性。
   c. 每年於年底均會做災難復原測試的演練，以測試系統是否能如期恢復運作。
4. 機房的安全管控:
   a. 獨立的機房，出入均需資訊相關人員才能進出，並搭配監視系統及保全系統監測有誰進出。
   b. 配置滅火器，遇災害發生時能隨時使用，每月均需檢驗滅火器是否堪用，並填寫滅火器檢查表。
   c. 設立機房停電通知:如遇裝置停電時會立刻發出簡訊通知相關電腦人員，以便能立刻處置。
   d. 機房溫溼度:安裝溫溼度控制儀器，隨時偵測機房溫濕度，並由資訊人員每天兩次檢視後填寫於機房溫溼度檢測表。
   e. 獨立電源配置:由電氣室直接拉一條獨立的電力線到機房，並加裝穩壓器及 UPS，以確保電力的正常供應。
5. 資訊相關人員的安全意識:
   a. 不定時參加網路資訊安全研討會，以了解目前的最新資訊安全相關知識，來檢討改進公司的資訊安全是否能與時俱進。
   b. 資訊人員:為加強人員的資訊安全常識，須於每年參加資訊安全課程。
   c. 使用者端:由資訊人員來教育訓練相關電腦使用者端的安全意識。
6. 資安人員設置:
   a. 設置資安主管及人員各一位，並定期接受教育訓練
   b. 113 年 5 月參加台北資安大會一天
   c. 113 年 1 月參加資安系統專業人才培訓班五天
7. 防火牆合約三年(112 年 11 月到 115 年 11 月)
   112 年 11 月汰換購置眾至 NU-840H 防火牆一式，耗費 89,570 元