一、　資通安全風險管理架構

1. 喬山健康科技股份有限公司(以下稱本公司)已設置資訊安全專責主管及至少一名資訊安全專責人員，其隸屬單位「總部資訊」，負責集團資訊安全制度之規劃、監控及執行資訊安全維護作業。

2. 本公司資通安全監理之督導內部單位為”總部稽核及法務”，由該單位負責督導公司內部資通安全執行狀況，若有發現缺失，立即要求受查單位提出相關改善計畫與改進，並且定期追蹤改善成效，以降低內部資通安全風險。

3. 本公司資通安全監理之督導外部稽核單位為 與公司簽訂合約之會計師事務所，該外稽單位定期對公司資通安全規範、管理辦法與施行進行稽核，若有發現缺失，立即要求受查單位提出相關改善計畫與改進，並且定期追蹤改善成效，以降低公司資通安全風險。

二、 資通安全管理政策

1. 目的

為確保喬山健康科技股份有限公司(以下稱本公司)軟體、設備及網際網路之安全，維持業務持續運作，特訂定此資通安全管理政策，以達成資通安全管理的目標。

2. 定義

為確保各項資通系統免受任何因素之干擾、破壞、入侵或任何不當之行為，經由適當的系統規劃、程序規範及行政管理，以防範來自內、外部的威脅，達到維護資通系統安全，維持公司持續營運。

3. 目標

避免資通系統遭受來自內、外部人員不當使用或蓄意破壞，或當已遭受不當使用、蓄意破壞等緊急事故時，公司能迅速應變處置，並在最短時間內回復正常運作，降低該事故可能帶來之經濟損害及營運中斷。

4. 範圍

適用於本公司所有資通系統及其使用者。資通使用者係包含台灣總部以及全球子公司之正式員工、聘僱人員、建置暨維護廠商以及其他經授權使用之人員。

5. 組織

(1) 由總部資訊單位負責規劃資通安全、執行及相關事宜。

(2) 由總部稽核單位擬定相關內部控制程序管理及定期進行內部稽核。

(3) 由外稽單位定期對公司資通安全規範、管理辦法與施行進行外部稽核。

三、 資通安全具體管理方案

1. 人員資通安全意識及訓練

資訊單位需經常實施資通安全教育訓練及宣導，以提高人員對資通安全之認知及意識，並降低內部人為因素對資通安全之影響。

2. 資通系統安全管理

電腦主機、各伺服器等設備應設置於專用機房，由資訊單位負責管理，未經授權不可隨意進入；有因維護之必要進入，需由資訊單位人員陪同，並於出入管制表上登記。

3. 資訊機房維運

(1) 每日上班時間安排人員依”機房網路維運輪值點檢表”所列項目點檢有無異常，有發現異常時，依通報處理流程通知各級主管。

(2) 每日點檢 發現 有異常狀況發生時，應記錄於點檢表內的備註欄位，以供日後備查。

4. 資通系統及資料保護

(1) 每日上班時間，備份系統負責人員依”主機備份點檢表”所列項目點檢有無異常，有發現異常時，需檢查錯誤記錄，異常修正後，並重新執行備份。

(2) 每日點檢發現備份有異常狀況發生時，應記錄於點檢表內的備註欄位，以供日後備查。

(3) 各系統及資料備份需複製一份做為異地存放。

(4) 備份還原演練：

A. 每年按表訂時間進行還原演練，並將結果進行記錄。

B. 還原演練驗證後備份有效的版本需留存最新的版本至少一份，以做為最低資料毀損的保障。

C. 各系統負責人需完成每次還原演練測試後的處理程序修訂。

5. 資通系統及網路監控

(1) 各主機均列入監控系統監控，以監看各系統的運作狀態以及資源使用，確保各系統運作正常。

(2) 集團的網路均列入網路監控系統監控，以監看網路狀態以及各地頻寬的使用，確保各地網路頻寬以及網路效能正常。

(3) 當主機、系統以及網路異常時，監控系統會發送告警給相關人員，即時進行必要的問題處理或修復，以維持公司的營運。

四、 投入資通安全管理之資源

1. ERP 還原演練測試 + 會議，2 次/年

2. 各系統還原演練測試 + 會議，10 次/年

3. 郵件釣魚演練測試 + 會議，2 次/年

4. 郵件釣魚演練宣導，2 次/年

五、發佈時間: 民國 111 年 3 月 29 日