資通安全管理：

本公司成立資安風險管理小組，由資訊主管擔任召集人，定期檢討資安政策並向董事會報告，近期向董事會報告日期為 111 年 11 月 4 日，本公司於民國 111 年度並未發生任何危害電腦系統之重大資訊安全事件。

（一）資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源：

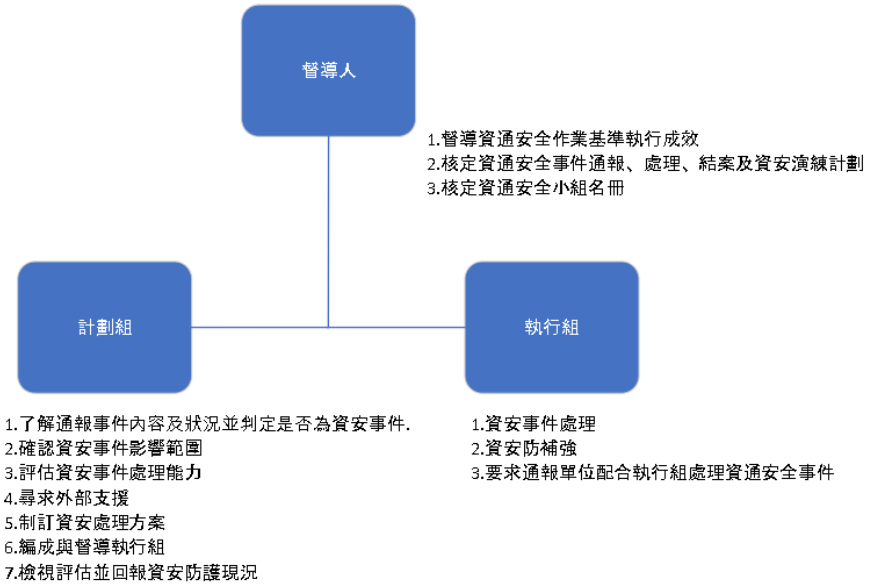
1.資訊安全風險管理架構

本公司資通安全治理組織之權責單位為資訊部，該部設置資訊主管，與專業資訊人員，統籌訂定企業內部資訊安全及保護相關政策、規劃暨執行資訊安全防護與資安政策推動與落實，並由企業資通安全組織最高主管定期向董事會彙報資安管理成效、資安相關議題及方向。

督導人：由資訊部單位主管擔任之

計劃組：由資訊部人員擔任之

執行組：由計劃組依任務需要編成之



2.資通安全政策

為使本公司各項資通安全政策能貫徹執行、有效運作、監督管理、持續進行，維護本公司重要資訊系統的機密性、完整性與可用性，特製定資通安全政策。

本政策旨在讓同仁於日常工作時有一明確指導原則，所有同仁皆有義務積極參與推動資通安全管理政策，以確保本公司所有同仁、資料、資訊系統、設備及網路之安全維運，並期許全體同仁均能了解、實施與維持，以達資訊持續營運的目標。

「落實資通安全，強化服務品質」

「加強資安訓練，確保持續營運」

「做好緊急應變，迅速災害復原」

- 落實資通安全，強化服務品質

  由全體同仁貫徹執行資訊安全，所有資訊作業相關措施，應確保業務資料之機密性、完整性及可用性，免於因外在之威脅或內部人員不當的管理，遭受洩密、破壞或遺失等風險，選擇適切的保護措施，將風險降至可接受程度持續進行監控、審查及稽核資訊安全管理制度的工作,強化服務品質,提升服務水準。

  加強資安訓練，確保持續營運

- 督導企業同仁們落實資通安全管理工作，每年持續進行適當的資通安全教育訓練，建立「資通安全，人人有責」的觀念，促使同仁瞭解資通安全之重要性，促其遵守資通安全規定，用此提高資通安全觀念及緊急應變能力，降低資通安全危害，以達持續運營之目標。

- 做好緊急應變，迅速災害復原

  制訂重要資訊資產及關鍵性業務之緊急應變計畫及災害復原計畫，並定期執行各項緊急應變流程的演練，以確保資訊系統失效或重大災害事件發生時，能迅速復原，確保關鍵性業務持續運作，並將損失降至最低。

3. 具體管理方案及投入資通安全管理之資源

本公司除建置安全的資通環境外並持續投入改善弱點提升系統作業效能，主要資通安全管理方案如下：

（1）網路安全攻擊風險說明與因應措施

一、 本公司建置網路安全防護管理，以確保企業內部營運相關資訊系統的運作，但是面對千變萬化的網路安全攻擊來源和手法，無法保證電腦系統能夠百分之百杜絕防止。

二、 針對工廠製造現場使用的電腦設備均隔絕連外網路或是採用封閉型的獨立系統，以避免網路安全危害事件導致生產線停止運作。

三、 主要營運用的IBM電腦主機都跟原廠簽訂長期的系統軟硬體維護合約，同時內部資訊系統維護人員亦熟悉資料備份與復原作業，確保電腦系統符合運作需要。

（2）本公司資訊安全控管措施如下

一、 網路安全監控：包含郵件伺服器(Email Server)系統以及公司網站之安全控管

A. 租用中華電信Hinet資安艦隊2018系列「新世代防火牆版」方案的專線服務，由Hinet執行網路安全監視工作，阻隔外

界駭客惡意的入侵行為，定期提供統計分析報表。

B. 入侵攻擊防護、網路防毒、反間諜程式、阻擋惡意連線IPS入侵偵測與漏洞防護，由Palo Alto 全球資安情資引擎定期自動更新特徵碼，偵測阻擋最新型病毒、蠕蟲、間諜程式、勒索軟體、挖礦軟體等惡意程式與連線，達到零時差防護。

五大類別網站控管

「惡意網站」，例如：惡意程式 (malware)、惡意釣魚(phishing)

「違反善良風俗」，例如：成人、嗑藥賭博裸露「降低生產力」，例如：社交網路、促銷拍賣股票與投資建議遊戲「影音播放」，例如：點對傳輸類、媒體與串流「其他」，例如：網頁型郵件服務、託管無法分類的站台

C. Hinet 除了提供網路安全控管的機制之外，在公司內部Internet 端口架設一台Firewall 設備，以監控及紀錄Internet 的各種使用狀況，提供警訊及必要的統計分析報表。

D. 郵件伺服器(Email Server)系統租用外部廠商提供的雲端郵件系統服務（Mail Cloud），由該廠商負責Email Server硬體維護與對外網路安全的控管，包括郵件防毒軟體服務，加強保護郵件的安全。

E. 本公司官方網站(www.nhjeans.com)系統委託外部的網站託管服務（Web Hosting），由該公司負責網站伺服器主機硬體維護與對外網路安全的控管。

二、 電腦安全：包含個人電腦與伺服器主機之連線控管、防毒與備份作業

A. 在內部網路(Intranet)或外部網際網路(Internet)，欲使用伺服器主機，必須透過安裝專用軟體，才能與伺服器主機連線。

B. 欲連線的PC(個人電腦)，必須在伺服器主機設定設備名稱，按需要性限制使用者只能在特定的設備名稱才能登入伺服器主機。

C. 任何使用者登入伺服器主機，作業系統OS(Operation System)都會隨時記錄登入日期時間和設備名稱，即使密碼錯誤也會記錄；使用者執行程式的過程也有相關的紀錄，退出主機的日期時間也有紀錄。

D. 欲登入伺服器主機時，密碼錯誤次數如果超過設定值，該User ID 和設備名稱將會被OS 暫停使用，唯有透過系統

權限管理者才能重新恢復。

E. USB 接口管制，沒有授權就無法使用USB 外接設備。

F. OfficeScan Console 防毒軟體主控台監管用戶端的更新和保護狀況。

G. 每日時執行伺服器檔案備份，包括磁碟對磁碟、磁碟對磁帶，多組磁帶版本並且異地存放。

三、 使用者安全：應用軟體系統安全控管

A. User ID(使用者帳戶)建立，由使用部門向資訊部提出申請，由系統權限管理者建立。

B. 執行連線軟體，必須要輸入合法之User ID & Password，才能進入應用系統使用者登入的畫面。

C. 按使用者所屬的部門別及所負責的職務特性，在不同的應用系統分別給予建立不同的User ID，其使用權限也特別區分。

D. 每一User ID的密碼，由使用者自訂，如果忘記，必須向資訊部提出更改申請，由系統權限管理者重新設定之。

E. 各部門人員異動或職務變動，必須向資訊部提出User ID權限的更改申請，由系統權限管理者重新設定之。

F. 使用權限按照 OS 提供的層級訂定，再配合不同應用系統的設定檔，進一步分別管理訂定。

（3）投入資通安全管理之資源

一、網路硬體設備如防火牆、備份管理設備、SSL VPN 私密通道連線。

二、軟體系統如郵件防毒、垃圾郵件過濾等。

三、資安人力：資訊主管一名及資訊工程師二名，每年至少召集一次資通安全管理的相關會議，負責資安架構設計、資安維運與監控、資安事件回應與調查、資安政策檢討與修訂。

四、執行狀況：每日各系統狀態檢查、每週定期備份及備份媒體異地存放之執行、每年資安宣導、每年對資訊循環之內部稽核、會計師稽核等。