一、資通安全管理目的：

針對目前資安新趨勢，如勒索軟體、木馬程式、社交軟體攻擊、偽冒網站等，透過專業合作及定期關注資安議題進行檢討因應規劃，以期能在第一時間偵測與阻擋，避免公司資訊安全暴露於風險中，同時定期向總經理及董事會匯報資訊安全治理狀況。

二、資通安全政策：

1) 建立資通安全風險管理機制，定期因應外在資通安全情勢變化，與合作廠商進行資通安全風險管控之有效性檢討，即時改善資通安全管理對策，以避免風險發生。
2) 制定"個人電腦使用管理"規章制度，針對個人電腦之使用管理、軟體支使用、移動儲存裝置與設備操作、網際網路之使用、郵件系統之使用安全等進行必要之規範。
3) 內部控制與稽核單位執行各項稽查，以確認資通安全管理有效落實執行到位，使資通安全之預防與管理有效性得以確保。
4) 不定期參與資通安全管理資訊交流，使資通安全觀念與作法沒有漏洞，且風險得以預防及控制。
5) 定期實施資通安全教育訓練，宣傳資通安全政策及相關更新政策與規定，確認所有員工具有資通安全意識，並配合資通安全政策落實。

三、資通安全管理方式：

本公司資訊安全之權責單位為行政管理處-資訊部負責，進行資訊安全政策規劃與執行，並由行政管理處副總進行督導，且定期向總經理及董事會告告資通安全治理狀況。管理規範說明如下：

1) 網路安全管理
   ①專職人員管理對外網路防火牆與監控，防止駭客入侵及病毒入侵。
   ②所有電腦登入帳密管控，並在防火牆設置相關政策，阻絕不當網址之連線，確保公司內部網路安全。
   ③所有電腦安裝防毒軟體，並定期更新，以防新型電腦病毒入侵。
   ④禁止使用 RDP 連線，以防止所勒索病毒攻擊。
2) 資料安全管理
   ①檔案伺服器權限控管，確保資料存取安全。
   ②定期進行資料庫及檔案伺服器資料備份。
   ③郵件檔案大小控管，避免大量資料外洩。
3) 裝置安全管理
   ①公司所有電腦安裝軟體控管，確保軟體使用之安全。
   ②USB 儲存裝置使用管控，防止惡意程式入侵公司內部網路。
   ③安裝防毒軟體，並定期更新，以有效防止病毒入侵。
4) 應用程式安全

①使用正版軟體，嚴格禁止私自安裝應用軟體。

②定期更新作業系統與軟體，避免惡意軟體利用系統或軟體漏洞進行攻擊與入侵。

5) 教育訓練與宣導

①辦理新人入職資訊安全教育訓練，說明公司資訊安全政策與規範。

②定期資通安全宣導，提升員工資訊安全意識。

③加強員工對電子郵件及社交軟體攻擊的警覺性，預防釣魚郵件及木馬程式攻擊。

四、資通安全管理投入資源：

本公司 111 年度投入資通安全管理資源，包含：軟硬體防護措施維護、新進員工資通安全教育訓練、配置資通安全專職人員、稽核單位定期稽查政策執行狀況。

五、資通安全管理未來精進：

為更有效率進行資通安全管控，與資訊安全落實，未來將規劃導入資料文件加密管理系統，以確保公司資料安全管理提升。