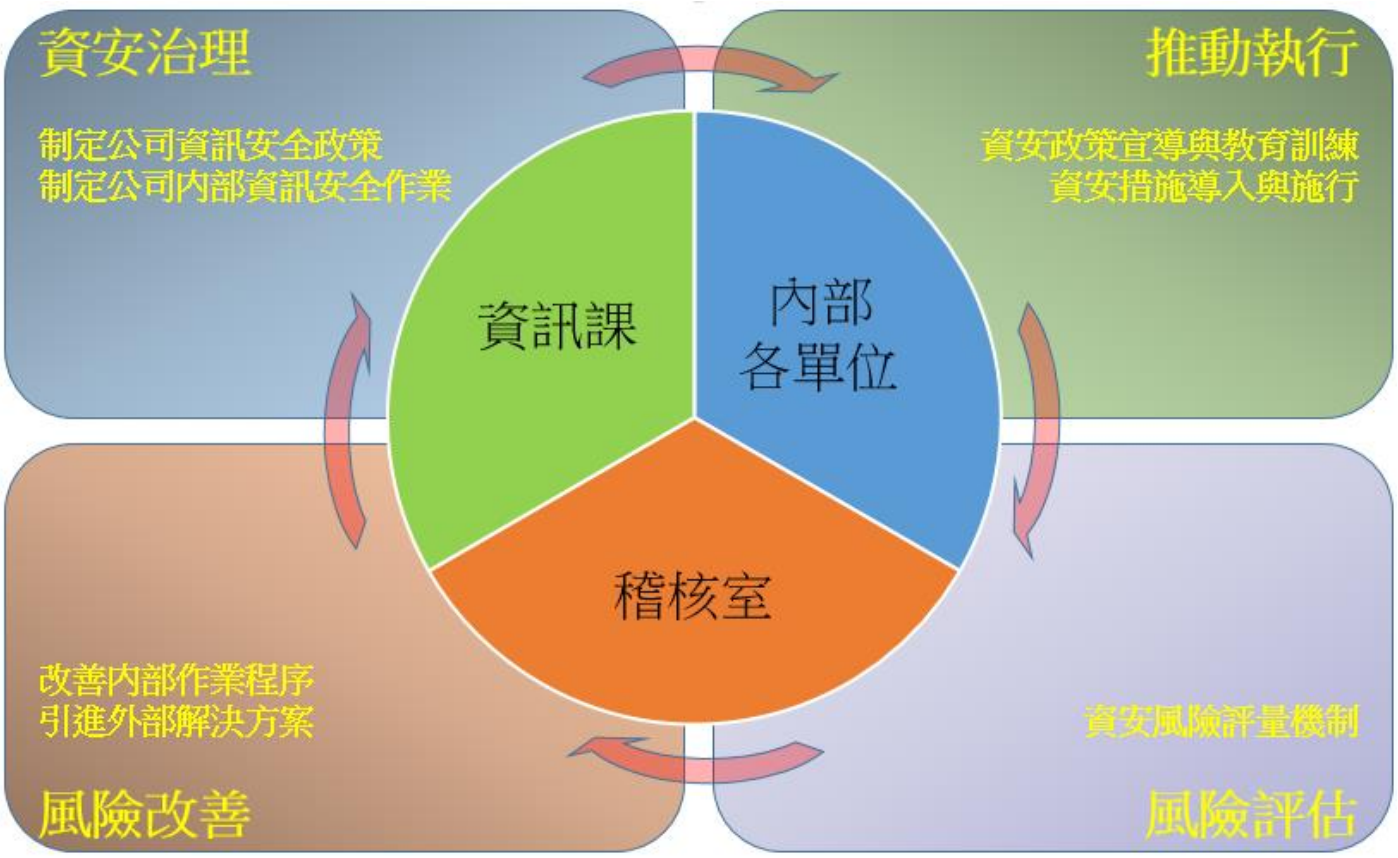
得力實業股份有限公司

資訊安全政策

資訊安全風險管理架構

- 本公司資訊安全之權責單位為資訊課，負責規劃、執行及推動資訊安全管理事項，並推展資訊安全意識。
- 本公司稽核室為資訊安全監理之查核單位，若查核發現缺失，旋即要求受查單位提出相關改善計畫並呈報董事會，且定期追蹤改善成效，以降低內部資安風險。
- 組織運作模式-採 PDCA（Plan-Do-Check-Act）循環式管理，確保可靠度目標之達成且持續改善。



資訊安全政策

為貫徹本公司各項資訊管理制度能有效運作執行，維護重要資訊系統的機密性、完整性、可用性，以確保資訊系統、設備網路之安全維運，達到永續經營目的。

本公司實施之資訊安全管理措施

資訊安全管理措施		
管理項目	說明	相關管理作業
資訊存取控制	管制公司相關資訊系統的使用權限與帳號管理	● 訂定系統存取政策及授權規定，並以書面、電子或其他方式告知員工及使用者之相關權限及責任。 ● 離（休）職人員，應立即取消各項資訊資源之所有權限，並列入離（休）職之必要手續。人員職務調整及調動，應依系統存取授權規定，限期調整其權限。 ● 建立系統使用者註冊管理制度，加強使用者通行密碼管理，使用者通行密碼之更新周期，最長以不超過三個月為原則。 ● 對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，並建立人員名冊，遵守相關安全保密責任。 ● 建立資訊安全稽核制度，定期或不定期進行資訊安全稽核作業。
主機安全措施與規範	維護公司內部主機及網路設備的安全以及正常運作	● 與外界網路連接之網點，設立防火牆控管外界與內部網路之資料傳輸及資源存取，並執行嚴謹的身分辨識作業。 ● 使用網路入侵偵測系統，監控網路流量，以確認未經授權而企圖上載或更改、網頁資訊或蓄意破壞者。 ● 裝設掃毒軟體，定期掃毒，以提供使用者更安全的網頁瀏覽環境。 ● 建立系統備援設施，定期執行必要的資料、軟體備份及備援作業，以備發生災害或儲存媒體失效時，可立即在新設備迅速回復正常作業。 ● 災害復原，不定期模擬駭客攻擊，演練發生安全事件時的系統回復程序，並提供適當的安全防禦等級。 ● 機密性及敏感性的資料或文件，不存放在對外開放的資訊系統中，機密性文件不以電子郵件傳送。 ● 自動接收所有來自相關作業系統廠商或應用程式廠商所寄發的安全維護電子信通知，並依照電子信的建議，安裝適當的修補程式（ PATCH ）。 ● 每日檢查各部主機及網路設備運行狀況，例如：主機或儲存設備面板系統指示燈，燈號是否異常、主機或儲存設備硬碟指示燈是否異常、各主機可用

		空間以及系統異常事件檢查、檢視各項網路設備系統指示燈是否異常、網路連線燈號是否異常。
防火牆之安全管理	避免公司內部主機及相關資訊系統遭外部駭客入侵與破壞	● 防火牆係整個網路之樞紐，對於防火牆主機及軟體，均應預留一套備份，以備不時之需。 ● 防火牆系統平時記錄整個網路之活動事件，記錄檔之資料至少應包括事件之日期、時間、起迄 IP 、通訊協定等項目，以便於平時之管理及日後之稽核作業。 ● 防火牆之記錄檔 (report) 由防火牆管理人員檢視分析有無異常狀況；記錄檔並應保存一年以上。 ● 防火牆主機只能在公司內部透過專屬的管理介面登入，不得以其他任何方式或公司以外的終端設備登入，以確保防火牆主機安全。 ● 防火牆之安全控管設定應經常檢討，並作必要之調整，以確定發揮應有的安全控管目標。 ● 防火牆系統定期作好資料備份，且只能做單機備份，不可採用網路等其他方式備份資料。 ● 防火牆系統軟體，經常更新版本，相關入侵偵測及病毒的特徵碼，每日定期更新，以因應各種網路攻擊。
資料備份作業原則	定期備份公司重要系統與資料	● 重要資料的備份，以維持至少三份並且放在不同儲存設備(含異地),且保留一個月為原則。 ● 備份資料有適當的實體及環境保護，其安全標準應儘可能與主要作業場所的安全標準相同；主要作業場所對電腦媒體的安控措施，應儘可能適用到備援作業場所。 ● 定期測試備份資料，以確保備份資料之可用性。
資料回復作業原則	發生突發狀況導致主機或儲存設備無法運作時,可迅速復原至其他主機或儲存設備	● 資料回復，除突發重大事件，主機機房或網路運作無法回復等因素外，資料能於 24 小時內回復正常，並保障備份資料能保持兩日以內之最新完整資料，資料回復後，程式及資料庫均能立刻正常啟用運作。 ● 資料回復作業完成後，相關單位人員應持續觀察三日，以確保系統運作正常，新增之資料正確無誤。
使用者電腦管理及宣導	降低公司內部電腦遭受病毒感染或資料外洩	● 每部使用者電腦，詳細記錄使用的人員及電腦名稱與 IP，並全部停用 USB 外接儲存設備，若臨時有需要複製檔案，經主管核可後，由資訊人員代為處理。

		● 每部使用者電腦均安裝防毒軟體，且管制使用網際網路，若有需求，填具申請單由主管簽核後，依據需求開放使用。 ● 不定期宣導相關資訊安全的注意事項，例如：如何判斷可疑的電子郵件、不開啟陌生郵件的附加檔案、客戶或廠商郵件內容有存疑，不直接原郵件回覆詢問，需透過其他聯絡方式再三確認等等。